WIPO Guide to Trade Secrets and Innovation

WIPO

WIPO Guide to Trade Secrets and Innovation

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

Suggested citation: World Intellectual Property Organization (WIPO) (2024). *WIPO Guide to Trade Secrets and Innovation.* Geneva: WIPO.
DOI: 10.34667/tind.49735

Cover: Getty Images/yucelyilmaz, FangXiaNuo

First published 2024

World Intellectual Property Organization
34, chemin des Colombettes
P.O. Box 18
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-805-3646-1 (print)
ISBN: 978-92-805-3647-8 (online)

Contents

Foreword

Trade secrets are arguably the oldest form of IP protection. Since ancient times, artisans and merchants have closely guarded their processes and techniques to maintain a competitive edge and protect their unique skills. Evidence of trade secret practices can be found in Hammurabi's Code of Laws, throughout the Roman Empire and among medieval guilds.

Despite this rich history, trade secrets have often occupied a rather dark and dusty corner of the IP toolbox, overshadowed by their more modern relations: patents, trademarks, industrial designs and copyright. Research shows that conscious and strategic usage of trade secrets is not widespread. Around 40% of SMEs provide no trade secrets training to their employees.

This is unfortunate. Most companies and research institutions, regardless of their size, business sector or location, have trade secrets assets, which if used savvily can help maintain a competitive advantage over competitors. A study by the Organisation for Economic Co-operation and Development (OECD) finds a positive relationship between the strength of trade secret protection in an economy and its innovation performance.

But there are signs that the perception of trade secrets is changing. Factors such as the rise of digital innovation, greater use of open innovation models, increased movement of talent and changes in patent prosecution are causing trade secrets to be deployed more and more as part of a healthy IP strategy. An age-old tool is being rediscovered.

The aim of this *WIPO Guide to Trade Secrets and Innovation* is to provide a comprehensive overview of the role of trade secrets in supporting innovation and knowledge sharing at the global level, whilst helping enterprises and entrepreneurs to incorporate them into their IP strategy.

Designed to be accessible and digestible, the Guide combines an overview of the relevant policy and legal frameworks, with practical insights and examples of the evolving role of trade secrets in today's economy. We illustrate how trade secrets can be used both as a defensive right, with chapters on management and litigation, and as a strategic asset for business growth and collaborative innovation.

Trade secrets have been hidden gems for too long. It is time to bring them into the light, so that they can truly sparkle. Whether you are a policymaker or business manager, a researcher or entrepreneur, we hope this Guide helps you to see the power of trade secrets and the value they bring to businesses strategies and global innovation.

Daren Tang
Director General
World Intellectual Property Organization

Acknowledgments

The preparation of the *WIPO Guide to Trade Secrets and Innovation*, including editorial work and design services, was funded by the Funds-In-Trust received from the Republic of Korea (FIT-Korea). The World Intellectual Property Organization (WIPO) expresses its sincere gratitude to the Government of the Republic of Korea for its generous and outstanding support given throughout the process, from the conception to finalization of the publication.

This publication was prepared under the general auspices of WIPO Director General Daren Tang, the Patents and Technology Sector led by Deputy Director General Lisa Jorgenson, as well as the Patents and Technology Law Division led by Andras Jokuti.

The WIPO Guide is the result of the invaluable collective efforts of WIPO colleagues, external contributors and peer reviewers.

The publication project was led by Tomoko Miyamoto, who oversaw the project, reviewed the contents, and was assisted by Nina Belbl. Fernando Cepeda Lacouture provided research assistance. Administrative assistance was provided by Elizabeth Day and Chittima Bunyasiriphant.

The inputs from external contributors, drawn from their practical experiences and insights in the business practice with respect to trade secret protection, have proven critically important in providing solid, reliable, and practical information. WIPO expresses its highest appreciation to the following external experts who provided textual contributions to certain parts of the Guide and also reviewed the final draft: Edoardo Barbera and Federico Manstretta (Bird & Bird, Italy) on Parts IV and V, Haakon Thue Lie (Dehns and Norwegian University of Science and Technology, Norway) on Part VI and Stephen MacKenzie (Koch Disruptive Technologies, United States of America) and Jonas Block (at that time, IPwe, Germany) on Part VII. In addition, Emmanuel Gougé (Pinsent Masons, France) provided valuable suggestions on the use of trade secrets in different sectors.

Furthermore, WIPO extends its gratitude to James Pooley (Lawyer, United States of America) for conducting a thorough review and providing numerous thoughtful comments. WIPO also benefitted from helpful suggestions received from Caterina Strippoli (International Chamber of Commerce (ICC)) through the peer review process. It also acknowledges invaluable comments received from Roger Kampf (World Trade Organization (WTO)).

In addition, the following WIPO colleagues reviewed the draft and provided substantive inputs to the draft: Todd Reves; Michael Mbogoro; Tamara Nanayakkara; Xavier Vermandele; Heike Wollgast, Lien Verbauwhede and Andrzej Gadkowski. WIPO colleagues in the Publications and Design Section as well as Web Communication Section also provided invaluable support and advice. The Division for Asia and the Pacific, in particular, Han Gyudong, facilitated the coordination relating to the FIT-Korea.

Part I: Introduction

In the dynamic and increasingly interconnected world of innovation and commerce, intellectual property (IP) protection plays a pivotal role in driving economic growth, fostering competition and promoting technological advancements. Among various forms of IP protection, trade secrets have emerged as a critical tool for businesses to safeguard their valuable confidential information and maintain a competitive edge in an increasingly global marketplace.

Responding to the increased global interest in the role of trade secret protection in knowledge creation and dissemination, the WIPO Guide to Trade Secrets and Innovation provides a global audience with comprehensive but digestible background material.

Beyond the description of the policy and legal frameworks of trade secret protection, the WIPO Guide also offers practical insights on effective management of trade secrets by businesses. Viewing trade secrets as an integral part of business assets of an organization, the Guide gives inspirations for strategic use of this relatively less explored field of intellectual property.

Accordingly, the targeted readers of the WIPO Guide include:

- Government agencies involved in patent and/or trade secret policies, innovation policies and capacity building and assistance in these areas
- Staff of WIPO Technology and Innovation Support Centers (TISCs)
- Staff of institutions dealing with technology support, such as technology transfer offices of universities and public research centers
- IP professionals who have not had an opportunity to work in the area of trade secrets but are willing to learn more about the subject
- Business managers involved in strategic creation and management of information assets
- Any others who are interested in IP strategy and management

The WIPO Guide may serve well for policy makers and managers from the business sector, universities and other innovation-oriented organizations to get the broad spectrum of trade secret-related issues and if need be, to easily find policy, law and practical information in sufficient depth. At the same time, the WIPO Guide can also be used as background material or a reference piece for anyone who is interested in IP strategy and management, because in practice, trade secret strategy and management are carried out in the broader context of IP and business strategy. Likewise, it can be used for general awareness, teaching and capacity building in this field.

After this introduction, the WIPO Guide is structured as follows:

- Part II Strategic roles of trade secrets in the innovation ecosystem

Part II discusses high-level goals of a trade secret system and its role in the innovation ecosystem, from the angle of fair competition, robust national IP strategies and improving efficiency of knowledge creation and sharing.

– Part III Basics of trade secret protection

This Part outlines the essential building blocks of the trade secret system. It informs the readers about the legal frameworks for trade secret protection and highlights the characteristics of trade secrets by comparing them with patents. In addition, it briefly touches upon how businesses use and leverage their valuable trade secret information.

– Part IV Trade secret management

Unlike traditional IP rights registered by authorities, trade secret holders need to actively manage their trade secrets to maintain their value and protect them from leakage and misappropriation. They also need to pay attention to the risk of third parties' trade secrets entering their knowledge system. Part IV takes a deep dive into the question as to how trade secrets can be managed to tap their maximum potential, with many illustrative practical examples and tips.

– Part V Trade secrets in litigation

Part V addresses the scenario where a trade secret holder detected potential trade secret leakage or misappropriation. Due to the fact that the core of trade secrets' value is secrecy, there are many unique challenges that arise in such a scenario. Pursuing litigation to obtain legal remedies is one option available for trade secret holders. Other options, such as alternative dispute resolution (ADR) mechanisms, can also be considered in certain cases.

– Part VI Trade secrets in collaborative innovation

Strategic partnership and collaborative innovation models are some of the key ingredients of a modern innovation cycle. As trade secrets also play an important role in cross-fertilization of shared knowledge and know-how, Part VI focuses on use and management of trade secrets in collaborative innovation, including collaborative research projects involving universities and public research institutions.

– Part VII Trade secrets and digital objects

Rapid advancement of digital technologies also has a considerable impact on which (digital) information we protect as trade secrets and how we protect trade secrets using digital means. Thus, Part VII discusses management of: (i) digital trade secrets in the form of, for example, digital data (text, audio, image etc.), algorithms or programming code; and (ii) trade secrets in any field that are stored in a digital format (for example, a recipe stored in a digital file).

In addition, the Annex to this Guide contains a list of reference materials that may be consulted by readers for more in-depth information.

Furthermore, to respond to the needs of readers who seek more in-depth information on certain topics, the web-version of the WIPO Guide published on the WIPO webpage on Trade Secrets, available at https://www.wipo.int/tradesecrets is accompanied by additional information.

The first supplement is an "Overview of Trade Secret Systems in Certain Countries and Regions." It summarizes the following aspects found in national/regional trade secret law: (i) sources of law; (ii) definition of a trade secret; (iii) scope of trade secret protection; (iv) exceptions; (v) civil remedies; (vi) criminal sanctions; (vii) procedural provisions; and (viii) trade secret protection in judicial proceedings.

The second supplement is trade secret management practices in different industry/service sectors. While the basic principles and TS management measures are in Part IV, there could be certain specific issues that may appear in different industry/service sectors. The second supplement therefore gives more nuanced pictures about trade secret management.

The contents of both supplements will be updated, or new contents will be added, regularly.

The WIPO Guide intends to capture the general commonality found in trade secret strategies, laws and practices that may be broadly applied to different countries and business sectors. However, there are important differences among national trade secret systems, and businesses set reasonable trade secret management measures case by case. Thus, the Guide is by no means an instruction manual or a prescriptive guidance. Rather, together with the supplemented information on the web-version, the WIPO Guide addresses common and different needs of a wide spectrum of readers.

Part II: Strategic roles of trade secrets in the innovation ecosystem

Topics covered in this Part:

- **Goals of trade secret protection**
- **The roles of trade secret protection in the modern economy and in innovation**
- **National policies and strategies relating to trade secret protection**

Protecting knowledge and know-how through confidentiality is very old. There are many examples in world history where the rulers, or persons who had lawful control over the information at that time, strategically used secrecy to create and maintain their economic gains – sericulture techniques, cotton-dyeing processes, glassmaking techniques, to name a few.

Some examples of how valuable business information was protected in ancient times reveal the essential nature of human business relationships. In Hammurabi's Code of Laws from 1754 BCE, it is ruled that if an artisan has undertaken to rear a child and teaches him his craft, he cannot be demanded back. However, if he has not taught the child his craft, this adopted son may return to his father's house.

While these historical anecdotes give us a few insights into the use of trade secrets, our interest lies in understanding the roles of trade secrets in the modern innovation ecosystem, which is very different from Hammurabi's time in many ways. Part II therefore highlights the high-level goals of the trade secret systems and their evolving roles in the modern economy, before looking into the specificities of the trade secret systems and their use, articulated in the subsequent Parts of the Guide.

1. High-level goals of trade secret protection

It could be said that struggles between those who want to control their valuable information through secrecy, on the one hand, and those who attempt to find them, on the other hand, have been found everywhere since ancient times. That might be the reason why the conceptual understanding of the protection of trade secrets has gradually been woven into distinct local social norms and law, in different ways. The national basis of trade secret protection currently ranges from relational obligations (contracts, employer–employee relationship, fiduciary duty of confidentiality etc.), property rights, unfair competition, or fairness and equity.

Nevertheless, it is possible to find general high-level goals of trade secret protection regardless of the national legal traditions and normative premises – why do we protect this particular species of confidential information?

To promote fair competition

In countries with market economy systems, **fair competition** between enterprises is considered as the essential means for satisfying the supply and demand of the economy, which also serves the **interests of consumers and society** as a whole.

Competition is one of the main driving forces of innovation. Since trade secrets are particularly vulnerable to misappropriation by others, protection of trade secrets against unlawful acquisition, use or disclosure suppresses anti-competitive business behaviors and aims to promote innovation through fair competition.

To improve efficiency of the innovation ecosystem

Protection of trade secrets aims to **improve the overall efficiency of the innovation ecosystem**. The need to keep information confidential in creating and maintaining competitive advantages continues to exist in modern times. Appropriate trade secret protection will lead both innovators and their competitors to invest in innovation activities as such in a more efficient manner.

For innovators, the availability of appropriate trade secret protection may reduce the need to invest in inefficient or costly behaviors, such as hiring only family members or confining all workers in an isolated island, as we know from history. It may also encourage competitors to invest in improving their capacity and competitiveness through lawful means, instead of spending their resources on bribery, espionage and other improper means of acquiring information.

For realization of commercial success, successful R&D alone is often not sufficient

Knowledge and know-how relating to developing and manufacturing products as well as marketing, sale and distribution of the products are necessary. In many service sectors, knowledge and know-how underpin the quality, cost and other factors that improve satisfaction of customers, which in turn differentiate a service provider from its competitors.

Trade secret protection aims to **promote creation of a wide range of commercially valuable information** that is important for businesses to generate revenue and maintain a competitive edge.

Seeing the above, the patent system and trade secret system have overlapping high-level goals. A fundamental difference between the two systems, i.e., a patent system based on public disclosure and a trade secret system based on confidentiality, does not conflict with sharing a common goal of supporting innovation and creativity for the benefit of the society. They simply try to achieve it in significantly different ways, in a complementary manner (see also Part III: Basics of trade secret protection, in particular, Section 3).

2. Evolving strategic roles of trade secrets in the modern economy

In this section, we will look at the roles of trade secret systems in the modern economy and innovation systems, characterized by globalization, speed, connectivity and a mix of open/closed business models.

2.1 Additional tool to navigate a globalized marketplace

In a globalized marketplace, businesses face intense competition from both domestic and international competitors. Trade secret protection provides certain safeguards in case of leakage or misappropriation of valuable confidential information.

As seen above, commercially valuable information for businesses is much broader than advanced technological information. Thus, trade secret protection provides a **level playing field** for market players in all sectors of all sizes, including the service sector and small local businesses.

2.2 Staying ahead of competitors

The rapid pace of technological advancements, coupled with the higher speed of information communicated among businesses and customers, has led to increased focus on protection of trade secrets to **stay ahead of the competition**.

Particularly in some sectors that sell products with a shorter lifecycle and a rapid shift in customers' preferences, launching products underpinned by trade secret protection ahead of competitors can provide a significant competitive advantage.

2.3 Supporting strategic partnerships and controlled diffusion of knowledge/know-how

Strategic partnerships and collaborations with other entities can be crucial for businesses to expand their reach and grow. In many instances, creation and delivery of products and services are the result of efforts of several independent operators and long value chains. To enhance the **efficiency of collaboration through cross-fertilization of knowledge and know-how**, sharing of confidential technical, business or commercial information with the partners may become important for both parties. Successful exchange of trade secret information held by collaborating partners and effective management of trade secret information generated by such collaboration are key to **open innovation** models that has been embraced by increasing numbers of organizations (see Part VI: Trade secrets in collaborative innovation).

While it may sound counterintuitive, trade secret protection may result in more knowledge diffusion through controlled sharing of knowledge than without such protection. Legal protection against misappropriation of trade secret information and legal remedies in case of the misappropriation can generate sufficient confidence and trust that are required by trade secret holders to share their vulnerable sensitive information with other parties, usually under certain conditions and subject to confidentiality agreements.

Relatedly, trade secret protection plays an important role in the **diffusion of knowledge and know-how in the context of employment** through, for example, an employer sharing trade secret information with certain employees. As it may entail conflicting interests of the holder of the trade secret information and the recipient of the information, national trade secret systems usually seek to find a balance between the two.

2.4 Filling a gap in the IP system and other mechanisms

It is widely recognized that IP is a tool that can facilitate innovation. Leveraging a patent system for extra normal return on investment is a general strategy for technology innovators. Other forms of IP also provide competitive advantages to businesses. However, they fall short of appropriately protecting information that derives its commercial value through secrecy.

One common mechanism to protect such confidential information is a contract to maintain confidentiality. However, contracts do not apply to people outside the contractual relationship, and thus cannot offer legal protection against misappropriation carried out by them through, for example, cyberattack or espionage.

Trade secrets fill these gaps, **complementing these other mechanisms** to safeguard the commercial value created by trade secret holders. They also provide opportunities for businesses to diversify their IP portfolios and protect a broader range of intellectual assets.

In practice, national economy is supported by various players: different industry and service sectors and entities with different levels of economic size and available resources. They utilize different ways of creating commercial value and financial income. Trade secrets can be relevant to all, due to the broad scope of information they can cover.

It is well known that a variety of appropriation mechanisms, which interact with each other in different ways, are employed case-by-case by businesses to protect their innovation. Accordingly, while no generalization is appropriate, some research papers suggest that trade

secrets are one of the most important appropriation mechanisms in some sectors - sometimes higher preference is given to trade secrets than patents in certain circumstances.

3. Trade secrets and economic growth: national strategies

Due to the confidential nature of trade secrets, in general, it is not easy to evaluate the effect of trade secret protection on innovation or economic growth based on sufficient data. That said, the assessment made by the Organisation for Economic Co-operation and Development (OECD) showed that there is a positive and statistically significant relationship between the strength of trade secret protection in an economy and that economy's key indicators of innovation and international economic flows in investment and trade. With a caveat that the positive relationship, drawn from a specific sample during a specific time and a specific range of variation, does not necessarily show causality and stated that ever stronger rights and remedies would not yield similar results, the report concluded that adequately protecting trade secrets may be an appropriate policy for strengthening certain aspects of economic performance.

From the perspective of national policies, the keyword found in the above conclusion appears to be an "adequate protection," i.e., an adequate national trade secret system that will achieve the high-level goals discussed at the beginning of this Part. Three aspects may be highlighted in this regard.

3.1 Synergies with other IP

First, in designing a national legal framework for trade secret protection, synergies with other forms of IP as well as other related areasof legal order (such as contracts, employees' rights and rights to information) may be considered. Since a trade secret system can potentially fill a gap in other laws and how they are used by local innovators, a trade secret law can complement them to assist local innovators to build their competitiveness, and therefore this may form part of the needs assessment.

Similar to other forms of IP, a holistic perspective is necessary to seek a balance among the interests of various market players, bearing in mind a wide range of information that can be protected by trade secrets.

For example, in accordance with the Unfair Competition Prevention and Trade Secret Protection Act of the Republic of Korea, the Commissioner of the Korean Intellectual Property Office (KIPO), in consultation with other relevant central administrative agencies, established the first Basic Plan for the Prevention of Unfair Competition and the Protection of Trade Secrets in 2021. The Basic Plan, which will be prepared every five years, aims to establish a foundation for innovation and enhance national competitiveness by strengthening the protection of trade secrets. Based on the Basic Plan, the Commission is also mandated to set and implement a yearly Action Plan, carried out by relevant central administrative agencies.

Likewise, although trade secret protection is not a mainstream subject in all national IP strategies, some countries also address trade secrets in conjunction with other forms of intellectual property, identifying the shortcomings in the implementation of trade secret law[1] or addressing trade secret protection as an important area for further development.[2]

3.2 Availability of remedies

Second, practical availability of remediesin case of misappropriation is one of the essential elements in a trade secret system. Many of the positive roles of trade secrets in innovation are set on the premise that trade secret holders have confidence and trust in the trade secret system, which includes the possibility of effective legal action against misappropriation. Beyond

1 National Intellectual Property Strategy of the Philippines 2020–2025. https://www.ipophil.gov.ph/national-intellectual-property-strategy-nips/.
2 National Intellectual Property Strategy of Brazil, Decree No. 10.886 of December 7, 2021. https://www.in.gov.br/web/dou/-/decreto-n-10.886-de-7-de-dezembro-de-2021-365433440.

the legal framework, legal professionals, such as local attorneys and judges play an important role in applying the law to concrete cases.

3.3 Management of trade secrets

Third, trade secret protection necessitates active engagement of the trade secret holdersin managing and maintaining the secrecy of the information so that it continues to be eligible to enjoy protection. In other words, to effectively protect their trade secrets, businesses need certain understanding about identification, management and protection of their trade secrets. Accordingly, some national authorities publish handbooks and guides that contain practical information for businesses, particularly for small and medium-sized enterprises (SMEs). They focus on how local businesses can use the trade secret system and benefit from it.[3]

Guiding enterprises in the protection and management of trade secrets in Singapore

As part of the Singapore IP Strategy 2030, the Intellectual Property Office of Singapore (IPOS) undertook a Study on the Protection and Management of Trade Secrets in Singapore in 2021 to gain a deeper understanding of Singapore's trade secret regime vis-à-vis other comparable economies. The study also sought to find out the level of knowledge and ability of enterprises in Singapore to protect and manage their trade secrets, and how they might be supported, especially in the era of rapid technological advances.

The study found that most enterprises recognized the importance of trade secrets for their business growth, with about 75 percent of enterprises considering trade secrets to be the most important to their business. However, about half of all enterprises were not familiar with Singapore's trade secret regime, and about 2 in 5 enterprises did not use any trade secret-related services. Most enterprises indicated that more can be done to support enterprises, including raising awareness of the importance of trade secrets and increasing the accessibility of trade secret-related services.

Accordingly, the Trade Secret Enterprise GuideTrade Secrets Enterprise Guide was commissioned by IPOS and published in 2022. The Guide is meant to serve as an introductory and practical reference for enterprises and includes non-exhaustive examples of available trade secret tools and services that enterprises may tap into.

Source: Trade Secrets Enterprise Guide, (IPOS), 2022, available at: https://www.ipos.gov.sg/docs/default-source/resources-library/trade-secrets/trade-secrets-guide.pdf

A well-designed trade secret system can play a strategic role in strengthening competitiveness of local businesses in a fair competition setting. Understanding the high-level goals of the trade secret system and impacts of trade secrets on local businesses is a starting point for policy makers to effectively leverage this unique form of protection and strengthen national competitiveness in an increasingly interconnected world.

3 For example, Handbook for Protection of Confidential Information - Improving Corporate Value, Ministry of Economy, Trade and Industry (METI) of Japan, Last updated in February 2024. https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf (in Japanese). An English webpage of METI covering information relating to the Unfair Competition Prevention Act is available at: https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html

Part III: Basics of trade secret protection

Topics covered in this Part:

- **What trade secrets are**
- **Legal frameworks for trade secret protection**
- **Trade secrets and patents**
- **Using trade secrets in business (essentials)**

This Part provides basic outlines of trade secret protection, focusing on the essential building blocks of trade secret systems. Reflecting the legal traditions of each country, national trade secret laws show differences in certain key areas. However, to provide a general overview of various trade secret systems, Part III particularly highlights the common areas in the national and regional trade secret systems, with references to international treaties, where appropriate.

For the country-by-country information, reference is made to the "Overview of Trade Secret Systems in Certain Countries and Regions"[1] and the Annex to this Guide, containing a list of reference materials relating to national/regional trade secret systems.

1. What are trade secrets?

1.1 Trade secrets in 150 words

In general, trade secrets are **confidential information**, which is:

- not generally known among, or accessible to, the persons in the relevant business sector (**"secrecy"**)
- commercially **valuable** because it is secret, and
- subject to **reasonable steps** taken by the rightful holder of the information to keep it secret, such as the use of confidentiality agreements for business partners.

Oftentimes, they are key components of an IP portfolio that strengthen the business's **competitive edge**. Like other IP assets, they may be sold or licensed.

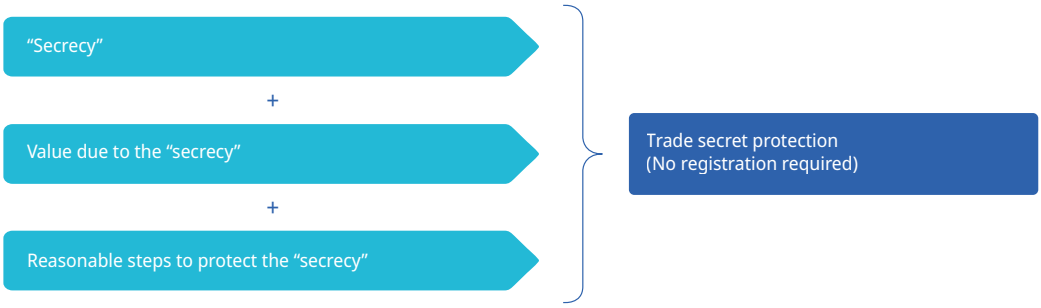
In principle, **unauthorized acquisition, use** or **disclosure** of a trade secret by others in a manner contrary to honest commercial practices is considered **misappropriation** of the trade secret.

If trade secret misappropriation happens, the trade secret holder can seek various **legal remedies**.

No registration is necessary to obtain trade secret protection. As long as the information qualifies as a trade secret, it is protected **indefinitely**.

1 https://www.wipo.int/tradesecrets/en/.

Figure 1. Trade secret protection



1.2 What kinds of information may be protected as trade secrets?

Patents protect inventions; industrial designs protect aesthetic designs; and trademarks protect signs or combination(s) of signs. In essence, trade secret protection applies to confidential "information," which can include **technical and scientific information**, **business and commercial information** as well as **financial information**. Basically, not only technical and scientific data and findings but also all kinds of ideas, strategies, data, know-how, techniques, methods of doing something etc. in the business and commercial sphere can be boiled down to "information," which we generate in our daily activities.

Therefore, practically, any information can be protected by trade secrets so long as it is "secret," has a commercial value because of the secrecy and is subject to reasonable steps taken to maintain secrecy. As long as these three criteria are met, a trade secret may also be made up of a **combination of elements**, each of which by itself is publicly known, but where the combination, which is kept secret, provides a competitive advantage, such as a secret process to produce a particular mixture of known chemicals.

Consequently, trade secrets are used in all sectors: not only in **manufacturing or technology** enterprises that offer products but also in those sectors that offer **services**, such as restaurants (e.g., recipes), garages (e.g., technique to wash and polish cars) and shops (e.g., customized advertising methods to keep customers' attention). As a tool to gain and maintain a competitive advantage vis-à-vis competitors, trade secrets are relevant to **businesses of all sizes**. In playing an important role in the innovation cycle from R&D to commercialization, **universities and research institutions** also started to pay attention to trade secret systems. Part VI: Trade secrets in collaborative innovation focuses on the role of trade secrets in collaborative innovation.

Valuable information can be stored in a mental memory and if necessary, be shared with others orally. In general, this mentally stored information can qualify as trade secrets. However, in today's business settings, much information is expressed in the form of texts, figures, drawings, charts, chemical formulae, diagrams, software code etc. and memorized on tangible media, not only in a written format but also in audio and video formats. In today's working environment, valuable information is predominantly **stored in digital form**, which gives rise to particular challenges for trade secret protection. Such issues relating to digital trade secrets are discussed in Part VII: Trade secrets and digital objects. Part IV: Trade secret management also addresses information technology (IT) security measures for trade secret protection.

In addition, what can be seemingly useless information, such as failed efforts to control adverse reactions of a particular substance to be used as a medicine or to overcome certain side effects or unsuccessful attempts to interest customers in purchasing a product, can be valuable trade secrets. Such information about failures **("negative" information)** may also have a competitive value, because once competitors know that information, they can save time, effort and resources by not having to try the same.

Table 1. Examples of information that may be protected as trade secrets

Technical and scientific information
Research and development methodologies and results
Engineering designs
Blueprints and prototypes
Manufacturing processes
Quality control methods
Product-related information (e.g.
Chemical formulae
Business and commercial information
Business
Business methods or service methods (e.g.
Sales and distribution methods
Suppliers' and customers' information (e.g.
Financial information
Internal cost structure and pricing information
Sales data
Salary and compensation plans
Negative information
Failed research
Details of failed efforts to solve problems in the manufacture of certain products
Unsuccessful attempts to interest customers in purchasing a product

1.3 How are trade secrets protected at national and international levels?

Unlike patents, and similar to copyright, trade secrets are protected without registration, that is, trade secret protection does not require procedural formalities and examination by national administrations. Therefore, trade secrets can be immediately protected in any countries where they meet the conditions for protection in these countries. While the great majority of countries apply the three conditions as illustrated in Figure 1, whether a particular piece of information qualifies as a trade secret or not in a certain country depends on the **applicable national law of that country**.

At the national level, trade secrets are protected by **common law and/or statute**. In some countries, trade secrets are primarily protected by the law of confidence, while in some other countries, they are regulated under laws that prevent unfair competition or specific trade secret laws. In the United States of America, each state has its own state law regarding trade secrets, while at the federal level, there is also a federal law that allows a trade secret holder to file a trade secret misappropriation claim in federal court.

In addition, since confidentiality agreements (or clauses) and non-disclosure agreements (NDAs) are usually effective measures to maintain trade secret information in secrecy, **contract law** is also relevant to trade secret protection. Furthermore, **employment law** is related to handling of trade secret information in the employer–employee relationship. Although some countries have

a long history of full-fledged national trade secret systems, many others have started shaping their national systems relatively recently, compared with other types of IPRs.

At the regional level, national laws of the member states of the European Union (EU) relating to trade secrets shall comply with the EU trade secret directive.[2]

At the international level, the history of normative developments on trade secrets had a sketchy record until the Agreement on Trade-Related Aspects of Intellectual Property Rights (**TRIPS Agreement**)[3], which binds all Members of the World Trade Organization (WTO) (see below).

Although it is not an international agreement that comprehensively covers rules relating to trade secrets, there are important principles that are generally accepted in many national laws.

- To enjoy trade secret protection, the above mentioned **three criteria** (i.e., secrecy, commercial value because of the secrecy, and reasonable steps taken by trade secret holders to maintain secrecy) must be complied with (see section 2.1 for the criteria to be met).
- Trade secrets can be protected for an **unlimited period of time**, unless they cease to meet the criteria for trade secret protection.
- Trade secret holders can seek protection only where unauthorized disclosure, acquisition or use of their trade secrets is made in a manner contrary to honest commercial practice. In other words, they **do not enjoy the type of "exclusive rights"** that are generally available for other categories of IP. This will be discussed in the next section.

TRIPS Agreement and Paris Convention: provisions relating to trade secrets

Article 39 of the TRIPS Agreement provides a minimum protection level of "undisclosed information," which WTO Members generally need to guarantee in their own legal system or practice. The term "undisclosed information" is generally understood as encompassing various terms (trade secrets, business secrets etc.) used in national legislations.

Article 39.2 states that so long as undisclosed information meets certain criteria, the lawful holder of that information shall have the possibility of preventing its undisclosed information from being disclosed to, acquired by or used by others without its consent in a manner contrary to honest commercial practices. A footnote clarifies the minimum scope of the "manner contrary to honest commercial practices" that the WTO Members must implement.

The Agreement also contains a provision (Article 39.3) on undisclosed test data and other data, the submission of which is required by governments as a condition of approving the marketing of pharmaceutical or agricultural chemical products which use new chemical entities.

In addition, Part III of the TRIPS Agreement (Enforcement of Intellectual Property Rights) applies to protection of undisclosed information.

In providing context for the protection of undisclosed information in the TRIPS Agreement, Article 39.1 refers to effective protection against unfair competition as provided in Article 10bis of the Paris Convention for the Protection of Industrial Property (Paris Convention).

Article 10*bis* of the Paris Convention states that the parties to the Paris Convention shall provide effective protection against unfair competition. The provision specifies that any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition. However, Article 10*bis* does not explicitly refer to trade secret misappropriation. Therefore, an express reference to that provision in the TRIPS Agreement established a formal link between protection of trade secrets and prevention of unfair competition at the international level.

2 Directive (EU) 2016/943 of the European Parliament and of the Council of June 8, 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. https://eur-lex.europa.eu/eli/dir/2016/943/oj.
3 https://www.wto.org/english/tratop_e/trips_e/trips_e.htm.

Note: Regarding Article 39.3, Paragraph 4 of the Ministerial Decision on the TRIPS Agreement adopted on June 17, 2022 during the twelfth WTO Ministerial Conference states that "Recognizing the importance of the timely availability of and access to COVID-19 vaccines, it is understood that Article 39.3 of the Agreement does not prevent an eligible Member from enabling the rapid approval for use of a COVID-19 vaccine produced under this Decision." Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/30.pdf&Open=True.

Modern trade secret laws are built on the TRIPS Agreement, which sets the minimum level of protection that WTO Members must implement. Therefore, in the subsequent Section, references to the relevant provisions of the TRIPS Agreement are added to assist readers. However, since Section 2 provides a general, non-exhaustive description of national/regional legal frameworks, references to the provisions of the TRIPS Agreement does not suggest any interpretation of the provisions concerned.

2. Legal frameworks for trade secret protection

2.1 Criteria for trade secret protection

Understanding of the three criteria that must be met for trade secret protection is important for trade secret holders because:

- businesses can avoid a mistaken assumption that the information they possess is a trade secret and spend their resources to maintain its secrecy
- it helps businesses to make informed decisions about the best way to protect their valuable information (for example, seeking patent protection)
- since there is no registration of trade secrets and no presumption of its validity, in a case where trade secrets are misappropriated, trade secret holders must prove that the information they possess meets these three criteria.

"Secrecy"

The first criterion is the "secrecy" of the information.[4] In general, information is considered secret if it is:

- not generally known or readily accessible
- within the circles that normally deal with this kind of information.

The "secrecy" element of trade secret law does not mean absolute secrecy - where only one person knows the information. In fact, the criterion of "secrecy" can be met if more than one person legitimately holds the same information (for example, they created the information independently) and guard it as confidential.

Or, as another example, if confidential information is shared with a business partner (or a limited number of business partners) under a confidentiality agreement prohibiting disclosure of that information, it is still "secret" information in the context of trade secret law.

It is also possible that even if the information pertaining to components of a body are publicly available, secrecy of the information covered by the body as a whole is still intact. For example, if source code is openly accessible and used by a company to develop other programs for other operating platforms, it is possible that the other programs can be considered "secret." The decisive point would be whether someone working in the field could readily access the newly developed program, not the initial source code. Similar consideration can be applied to assembly of components and configuration of systems.

Table 2 shows some examples of information that can be considered secret or, on the contrary, considered known or readily accessible.

4 See Article 39.2(a) of the TRIPS Agreement.

Table 2. Examples of information that can be considered "secret" or "not secret" in the trade secret frameworks

Generally considered "secret" information
A confidential list of customers compiled by ingenuity
A secret process or recipe to combine ingredients
Confidential manufacturing methods which you have shared with employees involved in manufacturing operations
A secret invention
Generally considered "not secret" information
Generally known
Self-evident information and knowledge that is generally known in the relevant industry or commerce
Public information in, for example, academic publications or published patent applications/patents, or on websites or marketing materials
Information given out at trade shows and conferences without a non-disclosure agreement
Information that can easily be ascertained from a product sold on the open market
Readily accessible
Information that can be easily compiled from more than one public source with a minimum of time and labor. For example, a list of potential customers interested in a certain product or service that can easily be reassembled from looking at information on their websites

As a logical consequence of this criterion, if trade secret information becomes known (published) or readily accessible to those working in the field, it may no longer be protected by trade secret law. For example, valuable technological information protected by trade secrets can be outdated at some point and generally known to those working in the same technology sector. Or, a competitor may create the same valuable information independently and publish it. In both cases, the trade secret information becomes "generally known," and the trade secret protection ends.

Finally, to those who are patent experts, it should be noted that the "secrecy" required for trade secret protection must not be confused with the notion of "novelty," "prior art" or a "person skilled in the art" in patent law. The "secrecy" required in trade secret law is distinct from these notions in patent law.

How to prove the "secrecy" (or non-secrecy) of information in litigation is discussed in Part V: Trade secrets in litigation, in particular, in Section 4.2.

Commercial value due to "secrecy"

The second criterion is that information must have commercial value because it is secret.[5] Information can only constitute a trade secret if it has **commercial value**, which usually brings some **competitive advantage** to its holder. This advantage must **derive from the "secrecy"** of the information and not from other reasons, such as quality, completeness or relevance of the information.

The requirement of commercial value of information and competitive advantage for businesses does not necessarily mean that the information as such directly brings income to the holder of the information.

– "**Negative information**" (see 1.2) might have commercial value vis-à-vis its competitors.

5 See Article 39.2(b) of the TRIPS Agreement.

– In some instances, the fact that competitors or consumers may **perceive** the information as valuable because of its secrecy may be sufficient to give its holder a competitive advantage.

Similarly, whether the information was obtained after extensive research incurring tremendous cost is not important for meeting this criterion.

Generally, the commercial value can be **actual** or **potential**. To demonstrate the latter, there must be some reasonable expectation of commercial or economic value in the future due to secrecy. Thus, practically, information acquired during an R&D process may also possess potential commercial value, even if its future success is uncertain.

Some examples of information that can be considered fulfilling (or not fulfilling) the criteria of commercial value due to secrecy are listed in Table 3.

Table 3. Examples of information that can have commercial value due to secrecy (or not)

Commercial value due to secrecy	Commercial value due to secrecy
"Yes"	"No"
A new process that allows your business to produce its goods or provide its services in a more cost-effective manner, or to offer more attractive prices, because competitors do not know that process.	Old or obsolete information if it no longer can be reasonably expected to provide commercial value.
A secret that gives your goods or services a higher quality than your competitors' products or services.	Information that is too remote from business activities (such as scandalous information about the private life of a competitor).
R&D test results, showing that it is worth pursuing further development or commercialization.	
The results of lengthy and expensive research which proves that a certain method will not work.	

With changes in market conditions or in business strategies and directions, trade secret information can lose its commercial value for the trade secret holder, and hence its protection. For example, there is no trade secret protection for software code that can no longer be executed in a working system and provides no other value to the trade secret holder.

How to prove in litigation that the information possesses commercial value due to secrecy is addressed in Part V: Trade secrets in litigation.

Reasonable steps

As a third element, to obtain trade secret protection, the holder of the information must take **reasonable steps under the circumstances** to **keep the information secret**.[6] In other words, trade secret holders need to take such reasonable steps to obtain and maintain trade secret protection.

To maintain secrecy of trade secret information, in general, trade secret holders are expected to take **reasonable security measures**, such as controlling access to facility and introducing IT security measures like firewalls and passwords. If they share the trade secret information with others (for example, an employer with its employees, or a research company with a collaborator), they are also expected to take measures to prevent the recipients of the information from disclosing it, such as through systematic conclusion of **confidentiality agreements or NDAs**.

What steps are considered reasonable depends on the **circumstances of each case**. The factors that may be taken into account include:

6 See Article 39.2(c) of the TRIPS Agreement.

- the company size
- the type of information
- the economic value of the information for the company
- the estimated duration of time the value will persist (for example, high investment for installing security measure may be not appropriate if the commercial value of the information will not persist very long)
- the risk of theft/misappropriation versus the cost of mitigating such risk (for example, extremely sophisticated security measures may increase safety of the information, but may increase cost and decrease flexible internal work processes and work efficiency).

Following these factors, a start-up will generally not be expected to take the same secrecy measures as established resourceful companies that can afford higher investment in their security systems. However, the more important the secret information is for the company, the more effort generally needs to be put into maintaining its secrecy. Therefore, it is possible that a smaller company needs to put more effort in security measures of particularly important information than a bigger company for less important information.

Example of highly valuable trade secrets for small businesses

If a start-up in the street-food business has built its whole success on one secret recipe of a particular soup, the secrecy measures may be more severe than those of a bigger company for their next month's advertising campaign, which will be public knowledge as soon as it is launched.

In practice, simple measures such as raising awareness and continuous training of employees on trade secret matters, allowing access to trade secret information only when a person has a "need to know," setting physical access barriers, using anti-virus programs and firewalls, as well as including confidentiality and non-disclosure clauses in contracts often prove to be reasonable for maintaining the secrecy of trade secret information. However, as discussed above, the reasonable level of sophistication should be determined on a case-by-case basis.

In addition, what can be considered as reasonable steps to maintain secrecy may change over time, also reflecting developments in the external environment, such as the rise of teleworking and development of digital technologies.

In a way, since trade secrets derive their value from secrecy, it is in the interest of trade secret holders to take measures to maintain secrecy of the information and properly manage their trade secrets in an efficient and effective manner. How to do this – a topic of **internal trade secret protection policies** and **trade secret management** – is discussed in detail in Part IV: Trade secret management.

2.2 What are the protections that trade secret holders may enjoy?

Trade secret protection does not grant exclusive rights on the protected information, but regulates the behavior of parties and prevents others from engaging in wrongful conduct that is against honest commercial practice. In essence, when unauthorized third parties acquire, disclose or use trade secret information with unlawful, improper, dishonest or unfair means, it is deemed misappropriation of trade secrets.

Specifically, trade secret holders, who can be natural or legal persons, shall have the possibility of preventing their trade secrets from being

- **disclosed** to others
- **acquired** by others, or
- **used** by others

without the holder's consent in a **manner contrary to honest commercial practices**.[7]

In other words, if an individual or a legal entity caries out the above actions the trade secret holder can file **lawsuits** against these actions (i.e., against **trade secret misappropriation)**.

No exclusive rights

In general, a trade secret owner cannot prevent others from independently developing and acquiring the protected information on their own and from using or disclosing that information. This is because conducting one's own R&D or own market analysis etc. to develop valuable information is usually deemed honest commercial practice. However, once a patentee X obtains a patent on its invention A, in principle, another person Y using the same invention A infringes the patent, even if Y came up with the invention A independently by its own, without any knowledge of the invention of the patentee X. Therefore, trade secret protection does not confer exclusive rights like patent protection does.

What is meant by "a manner contrary to honest commercial practices" depends on the applicable national or regional laws. Article 39, footnote 10 of the TRIPS Agreement, however, provides a useful clarification regarding the scope of practices that are "contrary to honest commercial practices." They are, *at least*:

- practices such as **breach of contract**, **breach of confidence** and **inducement to breach**, and
- **acquisition** of trade secrets by **third parties** who **knew**, or were **grossly negligent** in failing to know, that such practices were involved in the acquisition.

From the above, first, trade secret protection covers not only the misappropriation by persons with confidentiality relationships (e.g., contracts) but also misappropriation of confidential information by third parties outside such relationships.

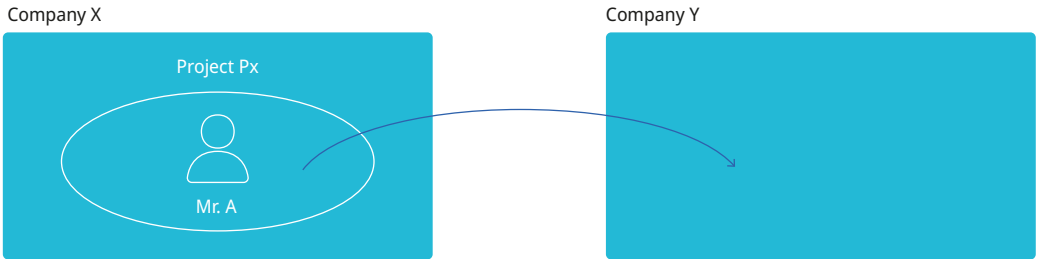
Second, as to third parties, trade secret misappropriation includes acquisition of trade secrets by a third party who knew, or was grossly negligent in failing to know, that practices contrary to honest commercial practices were involved in the acquisition of the information. Conversely, if a third party acquires the trade secret information without knowing, or without gross negligence, that the information is a misappropriated trade secret (i.e., **acquisition** of a trade secret by a **good-faith recipient**), their acquisition of the misappropriated trade secret is usually not considered as trade secret misappropriation.

Example of trade secrets acquired and used by third parties

Let's imagine the situation where an employee (Mr. A) acquired a trade secret of his employer (Company X) to carry out a research project (Px) that is expected to contribute to significant improvement of Company X's products. The valid employment contract concluded between Mr. A and Company X stipulates Mr. A's obligation to keep the trade secrets of Company X confidential beyond the termination of the employment contract.

Mr. A left Company X and was hired by a competitor, Company Y. Wanting to impress his new employer, Mr. A disclosed the trade secret information of Company X to Company Y.

7 See Article 39.2 of the TRIPS Agreement.



Did Mr. A misappropriate the trade secret?

Mr. A was bound by a contractual confidentiality obligation. Thus, his disclosure of the trade secret was in a manner contrary to honest commercial practices, and was misappropriation of the trade secret.

Did Company Y misappropriate the trade secret?

The answer may depend on the specific situation of the case.

- If Company Y knew that Mr. A misappropriated trade secret of Company X, the acquisition of this information by Company Y is also trade secret misappropriation.
- Similarly, if Company Y was grossly negligent in failing to know that the information acquired from Mr. A is a misappropriated trade secret, the acquisition of this information by Company Y is also trade secret misappropriation.
- For example, Mr. A openly told Company Y that he had acquired the trade secrets of Company X relating to Project Px, although he did not tell the exact content of the trade secrets. In addition, without hiding his hostility to Company X, Mr. A was very keen on working on Company Y's similar research project (Py). Knowing them all, Company Y assigned Mr. A to work on the project Py, without paying any attention to the risk of Mr. A using the trade secrets of its competitor. In such a case, if Company Y ultimately acquired the trade secrets of Company X from Mr. A through his activities in Project Py, most likely, Company Y should have known that the acquisition of the information involved the misappropriated trade secret of Company X.[8]
- However, if Company Y could not have known that Mr. A was disclosing and using the trade secret of Company X (for example, Mr. A concealed his professional profile and lied to Company Y), Company Y may be deemed a good-faith recipient of the trade secret information. In that case, acquisition of the trade secret by Company Y is not misappropriation of the trade secret of Company X.

Information, particularly valuable information, travels easily. Sometimes, the origin of the information is lost through transmissions or intentionally deleted. It is not always easy to trace the transmission of the information from one person to another. In some countries, therefore, **use or disclosure** of the trade secrets **by a good-faith recipient** could be considered trade secret misappropriation under certain circumstances.[9] For example:

- In some countries, once the good-faith recipients know (or should have known) of the previous misappropriation relating to the acquired information, the use or disclosure of information is no longer lawful.
- As a variant, in some countries, while the above principle applies, if the good-faith recipients acquired the information through a business transaction (such as a license), they are allowed to use or disclose the information within that transaction, for example, the execution of that license, regardless of their knowledge of previous misappropriation.

8 Company Y could have taken measures to prevent Mr. A from disclosing and using the trade secrets of Company X (and any other competitors), by, for example, using an on-boarding form that requires Mr. A to confirm his compliance with his confidentiality obligation with Company X (and others), as well as clearly instructing Mr. A to not to contaminate Company Y with trade secrets of Company X (and others).

9 The country specific information is available in the "Overview of Trade Secret Systems in Certain Countries and Regions", available at: https://www.wipo.int/tradesecrets/en/.

- As another variant, good-faith recipients are allowed to continue using the trade secret information, if they can show that it would be prejudicial to stop using the information, subject to a reasonable royalty set by the court.
- In some other countries, use or disclosure of the acquired trade secret information by good-faith recipients is allowed, regardless of their knowledge of previous misappropriation.

In some other countries, use or disclosure of the acquired trade secret information by good-faith recipients is allowed, regardless of their knowledge of previous misappropriation.

Products resulting from use of misappropriated trade secrets

Some countries explicitly legislate trade secret misappropriation relating to **products resulting from unlawful acquisition, use or disclosure** of trade secrets. In general, the act of making, selling, offering for sale, importing, exporting or placing on the market of such products amounts to misappropriation, if the person carrying out such act knew, or was grossly negligent in failing to know, that the trade secrets were used unlawfully.

Even if there is no statutory provision in this regard, in general, acts of exploitation of these products can be covered by injunction claims and other requests for relief in many countries.

When their trade secrets are misappropriated, trade secret holders must initiate actions to stop the misappropriation and seek remedies. This topic is addressed in detail in 2.4 below, and in Part V: Trade secrets in litigation.

2.3 Exceptions and limitation to trade secret protection

While improper, dishonest or unlawful acquisition, use or disclosure of trade secret information by unauthorized third parties is prohibited in principle, there are several exceptions to this principle. In addition, trade secret protection may be also limited in special relationships, typically, employer-employee relationships, to strike a balance between the interests of these two parties. The exceptions and limitations to trade secret protection vary among the jurisdictions.[10] Some of them are listed below.

- **Independent discovery**

Trade secret information does not cover independent discovery or development of the same information by a third party.

- **Reverse engineering**

In general, trade secret protection does not extend to acquiring trade secret information through reverse engineering, i.e., from examining a product placed in the market by disassembling, inspecting and analyzing the product to understand its mechanism, components, compositions etc. Note that, in some countries, a contract (for example, a purchase agreement) may forbid the recipient of the product to carry out reverse engineering.

- **Employee's skills and experiences**

Freedom to choose an occupation may set boundaries to trade secret protection. Employers' interests in trade secret protection beyond the employment period of their employees, and the mobility of employees, need to find a proper balance. Oftentimes, national contract law and labor law also regulate these issues. Depending on the national laws, employees' obligation to not disclose the employer's trade secret may be implied in the duty of loyalty of the employees.

10 The country specific information is available in the "Overview of Trade Secret Systems in Certain Countries and Regions." https://www.wipo.int/tradesecrets/en/.

Commonly, employers use contractual instruments, such as NDAs and confidentiality clauses, to control the use and disclosure of their trade secrets by employees. A non-compete agreement that restricts the possibility of an employee to compete with his/her employer even after the termination of the employment may prevent the employee from working with competitors after their departure. While it might reduce the risk of trade secret leakages, due to its highly restrictive nature, many jurisdictions prohibit non-compete agreements in principle, or their enforceability is subject to varied conditions and limitations, depending on the applicable national law.[11]

While certain restrictions on employees' use or disclosure of their employer's trade secrets are generally accepted in many countries, it is also widely understood that employees may use, in their post-employment activities, general knowledge, skills and experience that they acquired from the normal course of work with the (former) employer.

The issues relating to contractual agreements between employers and employees are addressed in Part IV: Trade secret management, Section 2.3.

– **Public interest and national security**

The basic notion that trade secret protection should not undermine the public interest is reflected in statutory law or case law of some countries.

However, it is a complex question, since public disclosure of trade secret information means that information is no longer eligible for legal trade secret protection. In this regard, the English court emphasized the difference between what may be of **interest to the public** versus what is in **the public interest to make the trade secret known**.[12]

Similarly, trade secret protection may be limited for the protection of essential national security interests, provided that the conditions in Article 73 of the TRIPS Agreement are met.

Example of public interest consideration

*Detroit Medical Center*v. *GEAC Computer Systems, Inc.*, 103 F. Supp. 2d 1019, 1024 (E.D. Mich. 2000)

Facts: Detroit Medical Center (Plaintiff) and GEAC Computer Systems (Defendant) were parties to a License and Maintenance Agreement ("Agreement"), which included a confidentiality clause preserving the confidentiality of the computerized inventory system (the "System") developed by the Defendant. Plaintiff entered into an Information Technology Outsourcing Agreement with Compuware Corporation, which in turn subcontracted with CareTech Solutions, Inc. This last subcontract would allow CareTech access to the Defendant's System, in violation of the Agreement. Defendant thereafter ceased providing its maintenance and support services. Plaintiff sought an injunction to compel Defendant to comply with the terms of the Agreement.

Holding: The court directed the Defendant to provide confidential access to CareTech, while considering the following factors:

- Potential harm to others – since the Defendant was willing to grant CareTech access to the System, provided certain conditions were met, any potential harm that could come from a preliminary injunction would be mitigated by imposing appropriate conditions on the injunction.
- Irreparable injury – without a functioning system, the Plaintiff ran the risk of not having adequate medical supplies and not being able to render sufficient medical services to the public.
- Public interest – while the Defendant argued that the public has an interest in the performance

11 Global Guide on Confidential Information, Trade Secrets and Post-Termination Restrictions, 2023, Bird & Bird. https://www.twobirds.com/en/insights/2023/global/global-guide-on-confidential-information.
12 Lion Laboratories Ltd v Evans [1985] QB 526, 537 (Stephenson LJ) citing Lord Wilberforce in British SteelCorporation v Granada Television Ltd [1981] AC 1096, 1168.

of contracts, the court held that public interest in adequate medical care outweighs general interest in confidentiality agreements, especially when the Defendant is willing to authorize disclosure under certain conditions.

– **Whistleblowing**

Relatedly, in some countries, trade secret protection does not extend to disclosure of trade secret information for revealing misconduct, wrongdoing or illegal activity. The exact scope of this exception depends on the applicable national laws.

To defend against misappropriation claims brought by trade secret holders, the alleged misappropriator may counterargue that their actions fall within the exceptions and limitations to the protection and thus are lawful acts under the applicable law. This issue is further addressed in Part V: Trade secrets in litigation, Section 5.2.

2.4 Trade secret enforcement

Overview

Even with the highest security standards, misappropriation of trade secrets by an employee, a business partner or an external entity can take place. Trade secret law provides a framework for trade secret holders to take legal action to seek remedies for misappropriation.

Due to the characteristics of trade secrets, there are several challenges that trade secret holders could encounter in trade secret enforcement.

- Since there is no authority registering trade secrets, the trade secret holder must **prove that they own** a "valid," protectable trade secret, and the defendant misappropriated that trade secret.
- Due to the confidential nature of trade secrets, **collecting evidence** of misappropriation is difficult. If the defendant is using the misappropriated trade secret, it is most likely that such use is kept confidential.
- If disclosure of the misappropriated trade secret has been made, or is likely to happen, the trade secret holder needs to take **immediate action** to prevent further disclosure to other parties. Once the trade secret is generally known to others in the relevant industry/service, its value to the holder will be lost.
- With a view to the **transparency of court proceedings**, trade secret information submitted to courts may be subject to public disclosure, depending on the applicable national law (see Part V: Trade secrets in litigation, Section 6 regarding preservation of trade secrets during court proceedings).
- National/regional trade secret laws particularly **vary in the area of enforcement**, reflecting differences in general procedural laws and legal traditions.

As an alternative to litigation, trade secret disputes may be settled amicably through direct negotiations between the parties or **alternative dispute resolution (ADR) mechanisms**, such as arbitration and mediation. Such consensual processes and amicable settlement of disputes are often desirable for commercial disputes, where preservation of future business relationships can be of high importance for both parties. At the same time, ADR mechanisms have their limitations. Thus, the best option for seeking remedies depends on the specificity of each case (see more on the ADR mechanisms in Part V: Trade secrets in litigation, Section 3.4).

More detailed information on trade secret enforcement is found in Part V: Trade secrets in litigation, which discusses, among other things, what practical steps can be taken by trade secret holders to enforce their trade secrets, what kind of remedies are available, who sues whom, how defendants may defend from misappropriation claims, handling of trade secrets in court proceedings, and cross-border issues.

Civil proceedings and remedies

Since the TRIPS Agreement addresses protection of undisclosed information as one of the types of intellectual property rights, Part III of the Agreement, "Enforcement of Intellectual Property Rights," also covers trade secrets. Accordingly, trade secret laws of many jurisdictions take into account the provisions of the TRIPS Agreement. The following paragraphs list the enforcement measures that are most relevant to trade secrets and are found in many jurisdictions.

Request for evidence held by the other party

Upon request by a party, courts may order the other party to produce the evidence it holds. A requesting party generally needs to present reasonably available evidence sufficient to support its trade secret misappropriation claims and has to specify evidence lying in the control of the opposing party which is relevant to substantiation of its claims. Courts may also set, in appropriate cases, conditions that are necessary to protect confidentiality of the information held by the other party.[13]

In common law countries, pre-trial discovery is widely used for the parties to have mutual access to all relevant facts. In civil law countries, in general, evidence held by others may be obtained in a more limited form.

Safeguards of confidentiality in judicial proceedings

The important principle of transparency of court proceedings is often anchored in national constitutions. In trade secret misappropriation cases, however, open court proceedings could mean that trade secret holders may lose trade secret protection by seeking judicial remedies against misappropriation. A proper balance needs to be found for the delivery of justice.[14]

Such safeguards may be important not only for protecting the trade secret of the plaintiff (trade secret holder) but also for the protection of defendant's (alleged misappropriator's) trade secret. For instance, in order to rebut the alleged misappropriation, the defendant may need to show that it also "owns" the same trade secret information that was developed independently.

Safeguards to protect confidentiality in the court proceedings depend on each jurisdiction. Commonly used measures include:

- exclusion of the public from the proceedings or *in camera* proceedings
- access to the sensitive information restricted to a limited number of participants (confidentiality clubs)
- publication of a redacted version of judgment, excluding the trade secret information.

National procedure laws

The procedural provisions regarding trade secret enforcement often refer to the general civil procedure law of the country concerned. In some jurisdictions, specialized courts have exclusive jurisdiction for trade secret misappropriation cases. Similar to other legal claims, in general, trade secret holders must take legal actions against misappropriation within a limited time period, often ranging between three to six years from the moment the holder knew or should have known of the misappropriation.

Provisional measures

Especially in trade secret misappropriation cases, trade secret holders seek provisional measures against the alleged misappropriator at the beginning of the case. Such quick action is often considered important for preserving the secrecy of the misappropriated trade secrets and the evidence held by the misappropriator.[15]

13 See Article 43 of the TRIPS Agreement.
14 See Article 42 of the TRIPS Agreement.
15 See Article 50 of the TRIPS Agreement.

Specifically, the plaintiff seeks a prompt court order to:

- prevent trade secret misappropriation from occurring, and in particular prevent entry into the channels of commerce in their jurisdiction of goods, including imported goods immediately after customs clearance; and/or
- preserve relevant evidence in regard to the alleged misappropriation.

In some instances, the effectiveness of provisional measures can be greatly compromised if a prior notice of the court order is given to the defendant. Thus, in especially urgent situations, such as where any delay in provisional measures is likely to cause irreparable harm to the trade secret holder, or where there is a demonstrable risk of evidence being destroyed, the judicial authority may grant an *ex parte* provisional measure without prior hearing of the defendant, if appropriate.

In ensuring a fair trial and justice for both parties, the judicial authorities usually require applicants for provisional measures to submit certain information or evidence. The applicant may also be required to provide a security, or equivalent assurance, to protect the defendant and to prevent abuse. There is usually a mechanism for review of the preliminary decision and if applicable, compensation to the defendant for any injury caused.

With a view to the temporary nature of the provisional measures, trade secret holders are usually required to start proceedings on the merits within a certain time period.

Remedies

Injunctions

The judicial authorities may order trade secret misappropriators to prohibit further acts of unlawful acquisition, use or disclosure of the trade secrets. Importation of products that result from trade secret misappropriation may also be prohibited.[16]

As explained in Subsection 2.2, above, whether a third party's use or disclosure of trade secrets that he/she acquired in good faith amount to unlawful act or not varies among different jurisdictions. Consequently, availability of injunctions in this regard depends on the applicable law.

Damages

The judicial authorities may order the trade secret misappropriator to pay damages adequate o compensate the injury the trade secret holder has suffered because of the misappropriation.[17] Courts may calculate the damages based on the profits made by the defendant, the plaintiff's injury (for example, loss of sales) or a reasonable royalty, depending on what is provided for under the applicable law.

The judicial authorities may also order either the plaintiff or defendant to recover expenses, including appropriate attorney's fees.[18]

Moreover, in some jurisdictions, punitive damages or treble damages are granted against a deliberate misappropriator who has behaved in a particularly daring manner.

Similar to the availability of injunctive relief, availability of damages against unauthorized use or disclosure of the trade secret by a good-faith third party depends on whether such act by the good-faith third party is excluded from the liability or not in the applicable law.

16 See Article 44.1 of the TRIPS Agreement.
17 See Article 45.1 of the TRIPS Agreement.
18 See Article 45.2 of the TRIPS Agreement.

Other remedies

In addition to the above, courts generally provide other remedies against trade secret misappropriation, taking into account the proportionality between the seriousness of the misappropriation and the remedies ordered as well as the interests of third parties.[19] They often include:

- destruction, or return to the trade secret holder, of any documents, materials or digital files containing trade secret information
- destruction of the products resulting from use of misappropriated trade secrets or removal of these products from the market
- destruction or removal of equipment used, or predominantly used, to manufacture the above products.

Criminal proceedings and sanctions

Many national laws provide for criminal sanctions in trade secret misappropriation cases.[20] The applicability of criminal sanctions to trade secret misappropriation is often limited to the most serious acts. The level of penalty usually depends on the severity of the misappropriation.

Even in cases where the applicable law does not apply penalties for trade secret misappropriation as such, oftentimes trade secret misappropriation is carried out with means that likely have criminal relevance, such as theft, fraud, coercion, electronic intrusion etc.

Depending on the applicable law, criminal proceedings can be initiated *ex officio* (i.e., on the initiative of the prosecuting authority) or at the request of the trade secret holder, or both. In some countries, the theft of trade secrets is only prosecuted upon request, notwithstanding that the prosecution authorities could, under the law, act *ex officio*.

3. Trade secrets or patents?

Trade secrets can be important intangible assets for business growth. They have many advantages compared to patents, but at the same time, their protection is more vulnerable compared to patents. Therefore, businesses usually use trade secret systems and patent systems in a **complementary** manner.

To illustrate the commonalities and differences between patents and trade secrets, Table 4 compares the main aspects of a patent system and a trade secret system.

19 See Article 46 of the TRIPS Agreement.
20 Article 61 of the TRIPS Agreement only obliges Members of the WTO to provide for criminal procedures and penalties in cases of willful trademark counterfeiting or copyright piracy on a commercial scale, but leaves open the possibility of WTO members to criminalize other cases of infringement, especially committed willfully and on a commercial scale.

Table 4. Comparison of patents and trade secrets

	Patents	Trade secrets
Subject matter	Inventions (technical feature)	Information
Criteria	Patent eligible subject matter	Secrecy
	Novelty	Commercial value due to secrecy
	Inventive step	Reasonable steps taken to maintain secrecy
	Industrial applicability	
	Sufficiency of disclosure	
Registration	Yes	No
Mandatory publication	Yes	No
Term of protection	Generally, 20 years from the filing date	Unlimited (if the trade secret criteria are met)
Protection	Exclusive rights	Protection against unlawful/improper/dishonest acquisition, use or disclosure
Protection against use by unauthorized parties	Yes	No, unless their use is in a manner contrary to honest commercial practices
Assignment	Yes	Yes
Licensing	Yes	Yes
Enforcement	Yes	Yes

3.1 Evaluating the appropriate type of protection

Listing these differences is not difficult. But answering the core question “How to choose which protection is better for me?” can be complicated.

For example, since trade secret protection is available without official registration, no administrative fees and/or fees for an attorney (or an expert, if allowed under the applicable law) to prepare and file an application are required. There is no need to wait for patent grant by the authority. On the other hand, as there are no such administrative procedures involved, trade secret holders must prove that they are indeed a legitimate holder of a protectable trade secret when they bring trade secret misappropriation claims to courts.

Similarly, in contrast to patent systems, trade secret systems do not require publication of valuable information by the authorities. However, trade secret systems do require trade secret holders themselves to be responsible for taking appropriate measures to maintain secrecy of the information concerned. These examples simply suggest that which protection is better for a specific piece of information depends on many factors, and ultimately, on both legal requirements under the applicable law and business objectives/resources of each organization.

From the outset, if your invention is not patentable, it may be protected as trade secrets in the form of confidential “information,” provided that it meets the criteria for trade secret protection (see the left column of Table 5, below). Firstly, since patent systems primarily protect technical features of inventions, they do not protect innovation that is purely of a business or commercial nature (e.g., a customer list). In addition, usually, patent laws specify certain inventions that cannot obtain patent protection. Secondly, inventions must meet the patentability requirements under the applicable patent law. Even if these requirements are not met (e.g., lack of inventive step), they might meet the criteria for trade secret protection.

Table 5. Underlying considerations for patent or trade secret protection

Invention is not patentable (may be potential trade secret)
Exclusions from patentable subject matter, e.g., plants or animal variety, essentially biological processes (other than microbiological processes), diagnostic, therapeutic or surgical methods for treatment of human and animal, discoveries, commercial/business, computer program as such
Inventions that do not meet the inventive step requirement
Invention is patentable (make an informed choice between patents and trade secrets) - examples of factors to be considered
Nature of the invention (product, process, predictability of the technology, reverse engineering, fast moving technology, etc.)
Competitiveness (likelihood of independent creation, reverse engineering)
Expected lifespan of the product (commercial value of the information longer than the term of patent protection?)
Cost of procuring
Opportunity cost (patent application published, but no patent grant)
Need to obtain exclusive rights? (fundamental up-stream innovation or incremental value)

When the invention meets the patentability criteria as well as the criteria for trade secret protection, a choice may need to be made between the two (see the right column of Table 5). Taking into account the advantages and disadvantages of both systems, several factors can be considered in making such a choice.

Nature of the invention

In general, information that can be easily acquired from the **product** put on the market would be difficult to protect under trade secret protection. However, **process** inventions (e.g., how to manufacture that product) may be carried out within the premises of the company that created it, making it possible to protect them as trade secrets.

Whether it is product- or process-related information, if third parties can discover it through **reverse engineering**, eventually trade secret information will be known to others and the protection ends. However, that does not mean that it should be protected by a patent, particularly where the **lifespan of the product** is short and "the first company in the market" (the so-called lead time advantage) is the most important element that determines the company's business success. In general, from the preparation and filing of a patent application to patent grant may take a few years.

Competitiveness

In general, if there is a likelihood of competitors being able to **create the same invention independently**, patent protection that enables patentees to prevent any third parties from making, using or selling the same invention would be more attractive than trade secret protection.

Expected lifespan of the product

If the lifespan of the product is expected to be longer than the term of patent protection, trade secret protection might offer a longer period of protection as long as the protected invention can be maintained secret, and it continues to have a commercial value due to its secrecy) during that period. At the same time, in practice, trade secret protection may be attractive only when it can be reasonably assumed that no competitors would be able to create the same invention independently, or no reverse engineering would reveal the confidential information.

Cost of procuring, maintaining and enforcing protection

As explained earlier, while there are no filing, grant and maintenance fees for administrative registration, trade secret holders need to take appropriate measures to maintain the information as a secret. In general, patent litigation can be expensive. However, seeking enforcement of

trade secret rights before courts can be also complex. In particular, trade secret holders may face challenges in collecting evidence and proving misappropriation of trade secrets.

Opportunity cost

In many countries, patent applications are published before the results of patent examination are known. If a patent application is rejected after publication, it is no longer possible to seek trade secret protection on the information contained in that application.

Need to obtain exclusive patent rights?

In some instances, the advantages gained from the exclusive patent rights may outweigh many benefits of trade secret protection. The possibility of preventing *any* third party from exploiting the invention can be considered extremely important for the competitive advantage of the business in some circumstances. This could be the case where, for example, the invention was created with high R&D cost and involves a foundational technology that would be expected to be used by others for many years.

Patent protection and trade secret protection are not always an alternative choice. In certain circumstances, these two protection mechanisms are used **concurrently**. Indeed, until a patent application is filed, an invention must be kept secret in order to avoid the invention becoming part of the prior art. In addition, it is often possible to file a patent application while holding as a secret information that is closely related to the claimed invention. In this sense, patent and trade secret protection may be viewed as **complementary**.

If the patent applicant maintains secrecy of the information about the invention even after the patent filing, trade secret protection continues until the publication of the patent application. Once it is published, its content will be generally known to the relevant circles and the trade secret protection will end.

4. Leveraging trade secrets in businesses

4.1 Importance of trade secret management

One of the peculiar features of trade secret protection is that trade secret holders need to take full control of their valuable information. Consequently, regardless of their sector or business model, trade secret holders should properly manage their trade secrets to maintain and strategically exploit those assets.

A **trade secret management program** that is well adapted to the trade secret holder's needs is essential. While it may include various steps, measures and processes, a high-level concept can be described as follows.

Figure 2. Trade secret management

1. Identify the most competitively valuable information in the business.
2. Identify the risks and impacts of any unauthorized acquisition, misuse, or accidental disclosure of the selected trade secrets, and of possible contamination by secrets of others.
3. Identify and apply risk reduction measures that are reasonable in relation to the value of the information, the level of risk and the cost of implementing various measures.
   For example, these measures may include:

   - education of employees about identification and handling of trade secret information
   - designation and periodical review of employees who "need to know" the trade secrets and restriction of access to only those employees

- physical and technological access restrictions
- limiting and monitoring public access to facilities that house trade secrets
- marking documents containing trade secrets as "secret" or "confidential"
- implementing computer system protections, such as passwords and firewalls
- securing confidentiality/non-disclosure agreements with relevant employees and outsiders who may get access to trade secrets.

4. Monitor and react to trade secret misappropriation and leakage.

In considering these four steps, there are several points that can be highlighted.

Management of your trade secrets and trade secrets of others

While protecting the company's trade secrets from leakage or external misappropriation risks is an important issue, how to avoid liability for misusing third parties' trade secret protection is an equally important concern for trade secret management.

Even if the company does not expect, or does not wish, to receive others' trade secret information, it can enter into the company's knowledge system via, for example, new employees, or through consultancy services. Once received without being noticed, it can spread very quickly and could be used widely in the company. Since new knowledge will be built gradually on existing knowledge, it will become difficult to separate and remove the trade secrets of others. In addition, receiving other's trade secrets via licensing agreements usually requires the recipient to take measures to maintain the secrecy of the information, as stipulated in the relevant agreements.

Reportedly, the higher risks for trade secret management are around employees changing jobs

Oftentimes, employers and departing employees have conflicting interests. Employers wish to prevent competitively sensitive information from being passed on to new employers, while employees wish to use their knowledge and skills to advance their career at the new employers or to start their own business. It can sometimes be difficult to separate these two classes of information, and the potential for misunderstanding can be quite high.

Beyond the legal framework set by trade secret law, labor law, antitrust law and contract law for example, experts often suggest that trade secret holders take operational precautionary measures, such as training and educational programs for employees, exit interviews with departing employees and monitoring any "signs" that might indicate potential trade secret misappropriation immediately before and after the employees' departure.

Conversely, new employees, particularly those involved in management and research, may unintentionally - and beyond the awareness of the new employer - use the trade secret information of their former employers to perform their new duties. Precautionary measures by new employers may include asking the new employees, as part of the on-boarding process, to confirm their commitment to not use or disclose former employers' trade secrets.

Another high-risk situation arises when trade secrets are shared with business partners, such as vendors, collaborative partners, and external consultants

Non-disclosure agreements and contracts with confidentiality clauses can be a very important tool to regulate handling of trade secret information in business collaborations.

For trade secret holders, monitoring the recipients' compliance with contractual terms may help them to address any potential issues at an early stage. The recipients of trade secrets, on their part, should be aware that receiving others' trade secrets usually brings new legal obligations as well as the risks of tainting their own information assets.

Furthermore, since the business relationship may change with time, reviewing and updating agreements should be in the interest of both parties. When trade secrets are shared in the

context of collaborative research, it is important for both parties to carefully define the rights of each regarding the newly created work, including jointly created trade secret information.

4.2 Strategic exploitation of trade secrets

Similar to other intellectual property assets, trade secret holders may:

- use the trade secret information **exclusively** by themselves, or
- **allow certain use of trade secrets by certain parties** under the control of the trade secret holder.

Usually, the aim of maintaining and exploiting trade secrets is to improve business efficiency and quality of products or services, with a view to attaining greater commercial success. To that end, trade secret information may be **shared** with, for example:

- business partners for collaborative R&D, marketing, and other projects
- local manufacturers of the company's products in foreign countries
- franchisees pursuant to franchise agreements
- external contactors conducting outsourced business processes
- external business or other consultants who provide advisory services.

The licensing conditions, such as the degree of authorized use of the trade secret (including after termination of the license) and the terms of payment, are agreed between the parties on a case-by-case basis.

In addition, legitimate control over the trade secret information may be **transferred to another party** against payment or any other conditions that may be agreed between them.

Furthermore, depending on the applicable national law, trade secrets may be recognized as collateral for raising capital from private or public institutions. They may be included in the company's accounting, contributing to its overall corporate value, or may be covered by a tax relief measure that aims to support innovation activities.

For the strategic exploitation of trade secrets, the following two points can be highlighted.

1. **Constant adjustment of trade secret exploitation strategy with changing business goals and needs.** Compared with other IP, trade secrets are very flexible assets – trade secret information can evolve together with daily business activities, and so can the scope of trade secret protection. The value of trade secrets is also affected by external factors, such as market trends and technological development. Therefore, the strategic exploitation of trade secrets is a dynamic concept that should evolve together with the organization's business goals.
2. **Exploitation strategy within and beyond the trade secret system.** Trade secrets can be used alone, shared with others or assigned to others. Particularly in the technology sector, trade secrets are part of the IP portfolio that, as a whole, is aimed at creating competitive advantage. Thus, trade secret strategy can be considered in conjunction with other IP rights. Section 3 of this Part already discussed different features of patents and trade secrets. With respect to software, in addition to patents, copyright protection may also be a possible protection measure. Both legal factors and business factors are relevant to maximize the value of trade secrets for commercial success.

Part IV: Trade secret management of this Guide navigates the reader through practical questions about trade secret management. In addition, Part VI: Trade secrets in collaborative innovation and Part VII: Trade secrets and digital objects address the potential of trade secrets to advance collaborative innovation and protection of digital technologies.

Part IV: Trade secret management

Topics covered in this Part:

- **Protection against misappropriation and leakages of trade secrets**
- **Protection against contamination with third parties' trade secrets**
- **Step-by-step trade secret protection plan and examples**
- **Situations with high-risk of misappropriation or contamination, exiting employees and hiring new employees**
- **Strategic exploitation and valuation of trade secrets**

1. Overview

Companies typically focus their attention on traditional IP registered rights, such as patents or trademarks, or other forms of protection, such as copyright for protecting their creative and innovative output. However, trade secret protection can extend beyond all of those. It can protect virtually any valuable information at relatively little cost. Almost all businesses rely on some sort of trade secret information, but many of them are simply unaware of their assets. Manufacturing processes, chemical compounds, prototypes, source code for software, food recipes, the process of making a perfume, customer lists, information on clients and their preferences, business models and marketing strategies: potentially, they can all be trade secrets.

Trade secrets can provide important benefits to their holders, in many different ways. They can be used by the trade secret holders, providing them with an advantage over their competitors. They can also be licensed or assigned, lead to public and private funding, attract investors and be shared in a joint venture. They may also give access to tax relief in some countries.

Trade secrets are therefore important assets for most companies, regardless f their size or industry sector. However, to reach their full potential, trade secrets need to be identified and protected. In practice, this is where trade secret management comes into play.

The ultimate goal of trade secret management is the maximization of the benefits that trade secrets confer on their holders in order to gain and sustain a competitive advantage over other competitors.

To pursue this goal, companies should focus on four main areas:

1. **Protection of trade secrets against misappropriation and leakages.** To preserve secrecy and maintain the company's competitive advantage, the trade secret holder should establish mechanisms for controlling access to confidential information.
2. **Protection against contamination from third parties' trade secrets.** To prevent from being targeted by third parties' trade secret misappropriation claims; information that comes into companies from outside should be treated cautiously.
3. **Strategic exploitation of trade secrets.** Companies should manage trade secrets in such a way that they increase enterprise value. This means understanding how trade secrets can be strategically used and exploited in the business.

4. **Valuation of the trade secrets.** Understanding the value of trade secrets that companies hold is important for taking informed decisions regarding both trade secret protection and exploitation.

Figure 1. Graphic representation of trade secret management

Against this backdrop, Part IV proceeds as follows. Section 1 provides an overview of the above four main areas. Section 2 provides guidance for setting up a trade secret protection plan aimed at preventing misappropriation and leakages of trade secrets. Section 3 addresses how to approach specific critical situations where the risks of misappropriation and leakages (i.e., outbound risks) are particularly high. Section 4 addresses the issue of protecting the company from contamination with third parties' trade secrets. Section 5 highlights certain scenarios where risks of contamination with others' trade secrets (i.e., inbound risks) cannot be ignored. Section 6 discusses how trade secrets can be strategically exploited, and stresses the importance of continuously aligning strategic use of trade secrets with business needs. Finally, Section 7 provides basic principles on trade secret valuation.

1.1 The subject matter of trade secret management

It is important to begin by clarifying terminology. Although "trade secrets" and "confidential information" are often used interchangeably in business, strictly speaking the former is a subset of the latter. In general, "confidential information" refers to information that is not publicly known and is kept confidential by its holder. Thus, it extends to information that is personal to an individual. Confidential information will qualify as a trade secret only if it meets the requirements under the applicable national law of each country (many of which may be based on Article 39 of the TRIPS Agreement).

In general, a trade secret refers to any confidential information which provides an economic benefit to the trade secret holder because that information is generally unknown to competitors, and the holder made efforts to keep the information secret. Trade secrets can be found in the most unexpected of places in your business.

Example of unexpected trade secrets

Company A produces substance X following a certain production process. Since it is an outdated process, many companies do not use it anymore. Company B, the major competitor of Company A, produces the same substance X, using a last-generation process. Company A does not want Company B and other competitors to know that it still uses the old process. Company A is sure that if Company B knew it, it would use this information to show how Company B is innovative compared to Company A. The old process itself does not qualify as a trade secret because it is widely known. But still, Company A has an interest in keeping secret the fact that it continues to use the old process. Therefore, Company A includes in its employee confidentiality contracts clauses that bind the employees to keep the information regarding specifically the production process of substance X confidential.

1.2 Protection of trade secrets against misappropriation and leakages

To protect trade secrets, the holder should set up a comprehensive protection plan that addresses at least two different questions:

- How to protect the company's trade secrets, to prevent trade secret leakages through employees and misappropriation by third parties.
- How to avoid third-party liability arising from the mismanagement of other's trade secret information that the company has legitimately acquired.

Example of protection of a company's trade secrets

Company A creates a bestselling sparkling drink. Competitors would like to know the recipe so that they can produce a similar product. Company A should take care to protect its beverage recipe from accidental leakages and willful misappropriation.

Example of avoidance of third-party liability

Company A develops a new and effective process to manufacture a certain product. However, Company A is not a manufacturing company, and therefore licenses the secret process to Company B. Company B is authorized to use the trade secret within the limits of the license agreement. Company B has to manage properly Company A's trade secret, in compliance with the license agreement and the law. For instance, if an employee of Company B disclosed the information to third parties (accidentally or willfully), Company B could be liable for the unauthorized disclosure of the trade secret.

For the information to be protected by trade secrets, in accordance with their applicable national laws, courts typically require, among other things, that the information has been subject to "reasonable steps" taken by the holder to keep it secret. Accordingly, using their own efforts and resources, trade secret holders should implement reasonable protection measures against trade secret misappropriation.

Reasonable protection measures

The reasonable protection measures are usually determined in relation to the value of the information, the level of misappropriation risk, and the cost of implementing various measures.

For example, theoretically and technically, intrusion to internal network systems can be prevented by cutting off any connection among computers or to external networks. But this sort of "extreme" protection is almost always impractical for modern businesses, which must communicate regularly with external actors, such as customers, vendors and joint venture partners. Indeed, it is widely believed that it is nearly impossible – from a practical and economic point of view – to protect each piece of information indefinitely, with the highest level of protection possible and under all the circumstances.

Therefore, reasonable protection measures do not always (and almost never) mean the strictest protection in the absolute, but instead the most effective protection according to the company's own risk environment and the specific circumstances of a given transaction. The level of protection can be set by identifying the trade secrets, understanding their value, weighing the risks inherent in the business, and prioritizing protection of the most important secrets, reaching a level of protection for each trade secret that is effective, proportionate and appropriate, according to the relevant circumstances.

Following this approach, the trade secret holder could decide not to protect certain information at all, or to protect it with less robust measures because the high cost (in terms of money or inconvenience) makes it impractical. For example, a company may decide that it is important

to allow broad and comprehensive access to an engineering database for all its engineers, to gain the benefit of collaboration among them, rather than to maximize security by limiting each engineer's access to the specific database that relates to their current work.

In this Guide, Sections 2 and 3 of this Part will focus on the protection of trade secrets from a management perspective, while protection of trade secrets in view of filing an action in court against trade secret misappropriation will be addressed in Part V: Trade secrets in litigation.

1.3 Protection against contamination with third parties' trade secrets

The second area of responsibility for trade secret management concerns the issue of how to avoid being contaminated by third parties' trade secrets. In other words, trade secret management addresses not only the "outbound" risk of leakage and misappropriation of the company's own trade secrets, but also the "inbound" risk of third parties' trade secrets entering the company unnoticed and being mixed up with the company's own information assets.

Contamination consists in the unwanted acquisition of trade secrets of third parties. It occurs, for example, when new employees bring with them information and documents of the former employer, and use them in the new employment, without knowledge of the new employer. Thus, the company has been "contaminated" with the other company's information.

Avoiding contamination with others' trade secrets is a distinctive area of trade secret management, representing potential harm to the integrity of a company's information assets, rather than possible loss of control. The company should design its trade secret management program such that it also protects against such risks of contamination.

Example of protection against contamination

Company A hires a product designer formerly employed at Company B. The product designer brings with him or her documents belonging to Company B and, once in the new role at Company A, he or she uploads the documents of the former employer in the data management system of the new employer. Also, eager to impress the new employer, the new employee uses them to inform the development of a new product for Company B. In such scenario, Company A runs a serious risk of being sued by Company B for trade secret misappropriation, together with the product designer.

Another example of potential contamination frequently arises when one company engages with another to explore a possible business transaction, such as a merger or a license and in the course of which discloses trade secrets. Here, the exposure to the other's sensitive information is voluntary and typically falls under the provisions of a confidentiality, or non-disclosure agreement. Unfortunately, the managers involved in such transactions may not be sufficiently aware of the risks involved in negotiating the terms of such agreements, or in complying with their terms. A great deal of preventable trade secret litigation arises due to insufficient management attention to these transactions.

Sections 4 and 5 will discuss the inbound risks of contamination and mitigation measures that may be taken, with more examples and practical tips.

1.4 Strategic exploitation of trade secrets

Once trade secrets are adequately protected against loss or contamination, they should be actively managed to support and increase the value of the enterprise. This is a crucial step toward commercialization that realizes the potential for competitive advantage represented by the information.

Like other IP, the trade secret holder should choose the best way of exploitation suitable for its business. For example, trade secrets can be used exclusively by the trade secret holder,

allowing the holder to offer a superior product or service or improve profit margins relative to its competitors. They can also be licensed, assigned, lead to public and private funding, attract investors, be shared in a joint venture or other form of collaborations.

Since trade **secrets are an integral part of IP assets**, their strategic exploitation should be considered in conjunction with other IP rights, such as patents. The value of trade secrets and risk of losing control over them constantly change together with the business activities and needs of the company and the evolution of external conditions, such as competition in the market, technological development and regulatory changes. Thus, the **optimal exploitation of trade secrets is a dynamic concept** that should be assessed, reviewed, and updated regularly so that it is constantly **aligned with the changing business strategy** of the trade secret holder.

In making an informed choice among different types of IP protection, both **legal factors** (for example, eligibility of protection, the scope of rights and their duration and geographical coverage), described in Part III: Basics of trade secret protection of this Guide, as well as **business factors** (such as costs, resources, market conditions and reputational effect) should be taken into account.

It is also possible that a rational business may decide to relax trade secret protection measures and also not to seek any alternative protection. Maintaining trade secrets is not an end in itself. They have value only to the extent that they provide a competitive advantage to the business, whether it is for technological competitiveness, monetary rewards or reputational advantage.

Section 6 will discuss in detail how trade secret holders may strategically approach exploitation of their trade secret assets by a third party.

1.5 Valuation of trade secrets

The exploitation of trade secrets is closely related to valuation of trade secrets, which can be very difficult for want of any meaningful market. But some form of valuation, either absolute or in relation to other assets, is often necessary, even if it is inherently inexact. For example, having some sense of the information's value may help to: (i) understand if it is worth investing expensive technological protection measures in the secret information; (ii) sell or license them to a third party; or (iii) quantify the damages suffered because of an unauthorized disclosure or improper use of the trade secrets.

Section 7 will illustrate primary valuation methods for IP assets, with their different strengths and shortcomings.

2. How to protect trade secrets from misappropriation and leakages? Trade secret protection plan

A trade secret protection plan can be broken down into the following four steps:

Step 1: Identify and value your "potential" trade secrets

Step 2: Determine the risks for your trade secrets

Step 3: Identify and apply reasonable measures to protect trade secrets

Step 4: Monitor and react to misappropriation and leakages.

The following sections will explain these four steps in detail. The outline of the four steps is contained in Sample checklist A: Implementation of trade secret plan – what steps to take, below.

2.1 Step 1: Identify and value your "potential" trade secrets

Trade secret protection plan (Step 1)

The first step to set up a trade secret protection plan is identifying the company's **"potential" trade secrets**.

Many organizations are unaware of the existence and the value of their information assets until they carry out a process to identify and catalog them. Companies may be surprised to discover extremely valuable assets that they didn't know they had. Thus, an internal review to identify potential trade secrets should be performed regularly.

The sub-steps to identify potential trade secrets are the following:

Identify the company's valuable information

Carefully review the company's competitive position to identify the information that helps the business run successfully and gives it an advantage over competitors. Consider the following steps:

Interview senior managers and key employees working in various functional areas and business units of the company. Questions could include:

- What makes your work different from those of competitors?
- What is the key to the success of your office or your team?
- What do you think competitors would like to know about your work?
- What do customers appreciate the most about the company's products or services?
- What causes you to lose sleep at night for fear that the competition may learn your secrets?

Analyze data on production, sales, customer satisfaction. This may provide useful information on the positive impact of new product or service offerings, business plans or marketing strategies. Particular attention should be paid to research and development, sales and business development functions, where there is often a higher concentration of valuable information.

Analyze competitors' products and customers' preferences to better understand how your secrets provide differentiated value over the competition. The result of this inquiry should consist of a broad set of the company's valuable information.

Select important trade secrets

Only a subset of the information collected under the first sub-step may justify implementing specific protective measures. In selecting information for particular focus, it is generally better to be over-inclusive, since both the risk and value factors can be dynamic, and you will want to preserve the option of caring for a larger set of assets. If the information is not known by the vast majority of your competitors, this should be sufficient to consider it a trade secret.

This "broad" approach could lead to over-classification, but some level of inconvenience is preferable to losing control of information that may later turn out to be critical.

Create a catalogue of the trade secrets

It is generally helpful to record trade secrets in some way so that decision-making can be easier and more predictable. However, trade secrets often consist of information which cannot be easily and quickly identified. Also, in large enterprises, information assets could be widespread among hundreds of employees, each developing, managing and using the know-how relevant

for their respective functions, which can change over time. Therefore, for management purposes, it is generally sufficient to draft a broad catalogue of trade secrets identified by category, including a brief description of why they are valuable for the company. The goal of such a catalogue is not to explain in detail all the company's information assets, but to raise awareness of these assets and improve decision-making about their protection.

Case example: "The Serve Machine 1100" – Step 1

The Super Tennis Racket Company is one of the biggest tennis racket producers worldwide. Its management, appropriately advised by the legal team, decides to monetize its information assets. To that end, the company appoints Louise to carry out a process to identify the company's trade secrets. Louise is the head of legal of The Super Tennis Racket Company, who has worked in the field for many years and knows the industry very well. As the initial step of the company's protection plan, Louise does the following:

Louise interviews the head of the manufacturing department who reports that since the company installed new machinery named "The Serve Machine 1100" to manufacture tennis rackets, product defects have reduced by more than 20% and the number of rackets produced per day has increased by 10%. Thereafter, Louise checks data from the customer care department: since "The Serve Machine 1100" has been installed, requests for replacements of rackets under warranty have reduced by 20%.

Louise asks Will, the head of the research and development team, about "The Serve Machine 1100": it was developed internally by The Super Tennis Racket Company. Louise asks Will to check if anything similar is on the market. The answer is no: "The Serve Machine 1100" is different. No one else uses something similar.

Louise fills in the trade secret catalogue as follows:

- *Item*: Tennis racket manufacturing machinery "The Serve Machine 1100."
- *Details*: Since its installation: (i) defective products have decreased by 20%; (ii) production has increased by 10%; (iii) requests for replacements of rackets under warranty has reduced by 20%. Developed internally. After preliminary search, nothing similar is on the market. Drawings and specifications remain secret. Valuable asset.

Louise hands over the catalogue to the management of The Super Tennis Racket Company, to discuss further steps. The management reviews the catalogue and realizes that "The Serve Machine 1100" is an important asset for the company.

Further steps are needed.

2.2 Step 2: Identify the risks for your trade secrets

Trade secret protection plan (Step 2)

After having assessed and catalogued the most important trade secrets, the holder should determine the risks that they face in the operation of the business. Understanding those risks is crucial to identifying the measures needed to mitigate them.

The major risks for trade secrets could be organized as follows:

- **Third parties' acquisition or misuse of the trade secret.** Businesses often attempt to gain access to information about their competitors. In general, lawful means of access may

include reverse engineering and independent discovery.[1] Competitors might also employ improper means, such as espionage or corruption of employees. Reducing that sort of risk is a primary objective of any trade secret protection plan. See Part III: Basics of trade secret protection of the Guide. In general, reverse engineering is a process of working backward from an available product, such as studying, analyzing or disassembling the product to understand its components, composition, design, functions or manufacturing process.

- **Leakages and accidental disclosures of the trade secret** One of the major risks of trade secrets is simple accidental loss because of negligence or mismanagement by those who "know" the trade secrets, e.g., employees or third party collaboration partners. Leakages and accidental disclosures can result from the practical difficulties of protecting the trade secret. For example, if exploitation of the information requires many people to know it, leakages may be more likely to occur. Other risks could be related to the specific medium on which the trade secret is fixed. Studies have shown that the greatest risk of secrecy loss is through mishandling by employees, which reflects the importance of proper communication and training of the workforce.
- **Trade secret misappropriation claims by third parties.** Given the high mobility of employees and of collaborations and other sharing arrangements in modern business, most companies face some risk of being accused of misappropriation. Such claims could arise either because the company is charged with directly misappropriating the trade secret, or because of unwanted contamination (see more extensively on contamination in Sections 4 and 5). Possible consequences of third-party claims include: (i) the need to defend against such claims, possibly in court; (ii) the need to stop, if the claims are grounded, the use of the trade secret (including the sale of the products and services using it); (iii) payment of compensation; or (iv) risk of criminal prosecution.

Potential risks, loopholes, and gaps in the protection of trade secrets can be identified through interviews with key managers and with those who deal with the trade secrets within the company on an everyday basis. External specialized consultants and security tests can help identify vulnerabilities.

For a thorough risk assessment, it is important to understand:

- the **likelihood that the potential risks materialize**, and
- their **potential impact**, i.e., the severity of their consequences.[2]

Indeed, annulling all possible risks is often impossible. What can realistically be done is to mitigate those risks, in particular prioritizing those with the highest probability of occurrence and with the most negative consequences. Managers, businesspeople, and representatives of those who will be impacted in their day-to-day work by the potential measures should be involved in the risk assessment and in the design of the protection program. Risk management measures are, in the end, the result of a balance of interests, where the need for security will be balanced with the need for efficiency and cost constraints.

The results of the risk assessment analysis should produce a risk assessment report that identifies the potential risks, the likelihood of their occurrence, their consequences and the priority level for intervention.

1 See Part III: Basics of trade secret protection of the Guide. In general, reverse engineering is a process of working backward from an available product, such as studying, analyzing or disassembling the product to understand its components, composition, design, functions or manufacturing process.
2 James Pooley, Trade Secrets § 9.03 [4], (Law Journal Press 1997-2023, updated).

Case example: "The Serve Machine 1100" – Step 2

Louise provided the management of The Super Tennis Racket Company with the trade secret catalogue, and they realized the importance and the value of "The Serve Machine 1100" for the company. The company therefore asked Louise to assess security risks related to the "The Serve Machine 1100." After some investigation, her findings are the following:

Risk 1 – Potential leakage

"The Serve Machine 1100" is very different from other tennis racket manufacturing equipment. However, the features that make their machinery so special can be easily identified and understood by a junior engineer or an experienced factory worker from an external analysis of the machinery. "The Serve Machine 1100" is located in an open area of the plant, where employees of all the departments have access. The Super Tennis Racket Company includes in all contracts of employment generic confidentiality clauses.

Risk assessment

- A high number of people have access to "The Serve Machine 1100" and a good part of them have also the knowledge to understand its peculiarities, even though most of them have no "need to know" about it to do their job.
- Many of the employees have been working with The Super Tennis Racket Company for many years, and likely they simply have forgotten that they signed a confidentiality clause many years ago.
- The level of protection currently in place at The Super Tennis Racket Company to protect the secrecy of "The Serve Machine 1100" likely does not meet the "reasonable steps" standard required by law. Therefore, in case of misappropriation of the technical features of "The Serve Machine 1100," it may not be possible to seek trade secret protection in court.
- The potential consequences of leakages could be very severe: competitors could acquire the technical information necessary to replicate the "The Serve Machine 1100," or such information could be publicly disclosed and destroy the secret entirely.

Risk 2 – Potential misappropriation

Roksana, a mid-level engineer on the research and development team who helped to develop "The Serve Machine 1100," revealed that she was recently contacted by the competitor The Bad Player for a job interview. At the interview, an engineer of The Bad Player asked Roksana how The Super Tennis Racket Company was able to improve the quality of its rackets. Roksana understood that The Bad Player was trying to have her disclose confidential information on the production process. She refused to answer and left the meeting. However, Roksana had the impression that The Bad Player clearly understood that there is a specific reason why the tennis rackets of The Super Tennis Racket Company have so significantly improved their quality, even if, apparently, they are not yet aware that the reason is "The Serve Machine 1100."

Risk assessment

- The Bad Player tried to acquire information on The Super Tennis Racket Company by targeting its employee. The Bad Player will likely try again to secure access to the information.
- The level of protection applied by The Super Tennis Racket Company is currently low, and therefore the chances that The Bad Player could reach its goal are high.
- The consequences are similar to those of Risk 1.
- The Bad Player has a bad reputation for its unfair business behavior. There is the risk that if The Bad Player succeeds in misappropriating the information, it could file a patent application in order to try to subsequently exercise exclusive rights conferred by a patent and prohibit The Super Tennis Racket Company from using "The Serve Machine 1100."

Risk 3 – Potential contamination

Roksana also referred to Caspar, an ambitious young engineer at The Super Tennis Racket Company who had also been part of the team that developed the "The Serve Machine 1100." Caspar arrived at the company directly from the research and development team of The Third

Set, another important competitor. Roksana was impressed by how much Caspar contributed to the development of "The Serve Machine 1100," despite his young age, and suspects that he had been working on something similar at his former employment.

Risk assessment

- Currently, there is no reason to believe that Caspar did something unlawful. He could simply be very good at his job.
- However, the circumstances related by Roksana suggest that Caspar may have misappropriated trade secrets belonging to The Third Set by using them to develop "The Serve Machine 1100." Should this be the case, The Super Tennis Racket Company would have been contaminated with The Third Set's trade secrets and risks facing claims of trade secret misappropriation.
- The company is considering investing money: (i) to increase protection of "The Serve Machine 1100"; and (ii) to build two additional versions of "The Serve Machine 1100."
- Before making this investment, additional investigation concerning the potential contamination is recommended.

Louise collects the information above in a risk assessment report. She concludes that the risks for the "The Serve Machine 1100" are overall high and actions must be taken with high priority.

2.3 Step 3: Identify and apply reasonable protection measures

Trade secret protection plan (Step 3)

Criteria to identify what protection measures are reasonable

After having identified the company's trade secrets, catalogued them, and analyzed their value and related risks, it is necessary to decide measures that are reasonable in relation to the value of information, the level of risk and the cost of implementing various measures – the most appropriate actions according to the specific circumstances of the case.

Broadly speaking, protection measures for a company's own information are directed at preserving secrecy and maintaining control over who has access to the information and what they are permitted to do with it. Considering all circumstances of the case, trade secret holders may take into account the following aspects to determine the reasonable protection measures.

The value of the trade secret

The more relevant the information is to the company's competitive success, the stricter the protection measures should be. The value of the trade secret is affected, *inter alia*, by the likelihood that the information remains secret and guarantees over time to its holder a competitive advantage over other competitors.

Characteristics of the organization

In general, the size of the organization affects the measures it can and should take, considering, for example, its resources and the level of complexity in managing secrecy within the organization.

The peculiarities of the business sector and the effectiveness of particular measures

The sector where the trade secret holder operates can also be relevant for the determination of reasonable protection measures. Some measures have general utility in all fields, while other measures are more effective in specific fields.

There are sectors such as personal insurance, where information on clients and their specific needs are key to the business, and therefore, contractual measures binding employees to confidentiality and practical measures related to education and training on trade secret management are of great importance. As a further example, employees in a sales or business development team selling customized industrial machinery components or supplying high quality fabrics according to the preferences of the clients, should be contractually bound to keep business information confidential. In highly technological sectors (such as the pharmaceutical industry, medical devices, automotive manufacturing and information and communication technology) or in sectors particularly exposed to cyber-attacks,[3] practical measures in the field of information technology are also very important.

The costs of trade secret protection

the budget of the company is often a critical issue, because protecting trade secrets can require significant investments in security measures. Generally, protecting a trade secret is sensible only if the investments in protection are lower than the expected economic return from the exploitation of the information. In this assessment, the progress of the technology over time should be considered, given the need and the costs of constantly updating relevant security measures. On the other hand, once an investment in general protection measures, such as a video-surveillance system and information technology controls, is made, often it can cover the cost of protecting multiple trade secrets at once, and newly acquired trade secrets can be protected by measures already in place. The costs may differ depending on the measure and the trade secret to protect.

Example of the costs of trade secret protection

Document management measures (such as a document marking policy) are generally low cost.

Logistics and organizational measures (such as a concierge service or video surveillance) may require high expenses, but they simultaneously protect trade secrets, physical assets and people.

Providing the company with **secrecy policies, codes of conduct, codes of ethics and specific procedures** can be expensive, since external consultants and lawyers may need to be involved. Basic policies and codes, however, can be drafted by the company's in-house legal team or otherwise prepared within a budget.

Training aimed at raising employee awareness regarding the importance of information security and their own responsibilities has variable costs according to the complexity, duration and recurrence. Basic training may be provided at low cost by the company's internal resources. In general, good training on confidentiality may be the most cost-effective way to reduce risk of information loss.

Contractual measures have variable costs depending on their complexity and the need to involve external lawyers to draft them. However, after an initial investment to get a fair insight

3 The four industry sectors appearing most affected by cyber theft of trade secrets are: manufacturing sector; information and communication technologies; financial and insurance activities; health and medical technology. See European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, The Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber, Publications Office, 2018, pp. 29-30. https://data.europa.eu/doi/10.2873/48055.

on a set of standard contracts and confidentiality clauses, companies may have sufficient internal resources to adapt them according to each specific case.

Information technology security measures entail costs that vary significantly, depending on the size and the needs of the company. Small businesses that conduct business on electronic devices can follow practical tips to keep IT systems safe and secure at low cost.[4] Multinational companies that manage a great amount of data, confidential documents and trade secrets in their data management systems should invest in sophisticated network strategies and cutting-edge measures to counter cyber-threats.

The need to maintain work efficiency

Some protection measures or their combination may affect the efficiency and fluidity of access to information within the company. A policy requiring multiple authorizations from multiple individuals every time the trade secret needs to be accessed may diminish the value of trade secret information by overly restricting its deployment in the business. Therefore, the need to protect trade secrets should be balanced with the need to exploit them efficiently through internal information flows. In this regard, it can be useful to interview the people involved in the workflows to assess possible alternatives and what measures can be realistically implemented without losing work efficiency.

Example of disproportionate protection

Company A has collected through the years a great deal of information on clients and preferences regarding customized industrial components that the company manufactures. Company A used this information to set up a very valuable database. The idea is that the business development and marketing teams can access the database to study the sales history of each specific client to make targeted offers to acquire new clients and improve customer service. However, for any access to the database, users have to: (i) ask for authorization from their supervisor, which is granted on average after two days; and (ii) explain the reasons for the requested access. To avoid cyber-intrusions, the database is saved only locally on a computer located in a dedicated room at the fifth floor of the headquarters of the company. The room is locked, and the key must be requested from the head of IT security, who requires signing a written confidentiality undertaking.

What are the results of this super-safe protection program? The business development and the marketing team, rather than having to comply with all these rules and procedures, simply performs their tasks without using the database, or creates a work-around that gives them access to some of the information, but without any ability of management to track that access. An important resource that could have provided a competitive advantage to the company remains unused, while sensitive data is used in insecure ways.

Balancing all the criteria above should suggest whether it is appropriate to protect any given trade secret and where to set the proper level of protection. Deciding that less valuable information should not be protected can be perfectly coherent with efficient management. Indeed, from a practical and economic perspective, it is generally not possible to protect all information with the same efforts, and it is therefore reasonable for the company to select only a subset of the information to actively protect.

4 For example, Information Commissioner's Office, 11 Practical Ways to Keep your IT Systems Safe and Secure. https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/11-practical-ways-to-keep-your-it-systems-safe-and-secure/.

Implementing protection measures

Finally, once the holder has identified the reasonable protection measures for each category of trade secrets, the last step is to implement those measures. Because they were developed thoughtfully in relation to perceived value and risk, those measures will also meet the flexible "reasonable steps" standard of protection according to law.

Usually, a trade secret protection plan consists of the implementation of a combination of operational and contractual measures. The following typical protection measures will be addressed in this section.

Operational measures

- **Setting up clear trade secret management roles and decision-making processes**: define clear roles and responsibilities within the company with regard to trade secret management and decision-making processes.
- **Document management measures**: handle information and documents properly inside the organization (e.g., policies regulating document classification and marking, a life cycle of documents and access authorization processes).
- **Logistics and organizational measures**: control and monitor access to the places where trade secrets are stored and used.
- **Education and training of employees**: provide education and training for employees, based on internal policies and a code of conduct or ethics, to raise awareness of their responsibilities in protecting trade secret assets.
- **Information technology measures**: use information technology security measures to secure trade secrets in transit and in storage.

Contractual measures

- **Internal with employees**: conclude contracts between the trade secret holder and the people internal to the organization, to bind them to confidentiality and other contractual obligations to preserve secrecy.
- **External with suppliers, clients and partners**: conclude contracts with external parties, such as consultants, contractors, vendors, customers, distributors, sales agents, actual or potential business partners, to bind them to confidentiality and other contractual obligations directed at limiting access to, or use of, the trade secrets.

Setting up clear trade secret management roles and decision-making processes

Trade secret management involves many critical management decisions, which might have to be taken quickly in some cases (e.g., reacting to trade secret misappropriation to prevent further dissemination or disclosure of the trade secret).

Therefore, roles and responsibilities of managers in the organization should be clearly allocated and the decision-making processes must be clearly set. For example, the following steps can be taken.

Establish clear roles and responsibilities

Make clear who has the responsibility for taking trade secret management decisions. Responsibility can be split according to the importance of the trade secret and the decision to make. High-level management might be involved in the most relevant decisions only. For example, whether to mark a specific document as confidential or not is something that can be handled internally within the business unit. Instead, whether to license the trade secret to a third party should require authorization from high-level management.

Clarify and streamline the trade secret management decision-making process

Specify when authorization for taking a trade secret management decision is necessary and how such authorization can be obtained. Consider setting up an ordinary procedure and

an accelerated procedure, the latter to be used only when authorization is needed on an urgent basis.

Appoint a "Trade Secret Officer"

Identify and train a person(s) to be available to employees when they need clarification, guidance or supervision in uncertain situations ("Trade Secret Officer").

Have an emergency plan in place

Set up an emergency plan, listing people to be contacted inside the company (executives and the Trade Secret Officer) and outside the company (legal and IT resources). Define the steps to be immediately taken or avoided in case of an incident. This plan can cover situations where the company finds misappropriation of its trade secret and where contamination with a third party's trade secrets is suspected.

Document management measures

Trade secrets often consist of information included in various kinds of records, for example, emails, memorandums, reports, business plans, contracts, client lists, technical documents, minutes of meetings, etc. They should be handled properly to avoid both accidental disclosure and unlawful acquisition, use and/or dissemination.

The main goals of internal document management measures are: (i) to make trade secrets recognizable by labeling; (ii) to make trade secrets difficult to misappropriate or circulate; and (iii) to make documents containing trade secrets traceable to easily identify authors of misappropriation or leakage.

In general, a golden rule for document management measures is that they should be **as simple as possible**, because if measures are too complicated, the risk is that the employees will simply ignore them, or bureaucracy slows down the operations. Some examples of document management measures are the following.

Document marking

Document marking is not always necessary to claim trade secret protection. However, it is **highly advisable** to adopt a document marking policy. Statements such as "*Confidential - Property of Company X*," "*Access limited to …*" or similar wording can be printed on documents.

Reference to the confidentiality level of the document (low, medium, high, etc.) and basic instructions on how to handle them (for example, not to be shared, not to be printed, not to be brought outside the company, not to be saved on certain media, to be encrypted) can also be included.

The task of marking documents with confidentiality labels should generally lie with the employee creating the document or circulating it within or outside the company. However, employees with specific training may be appointed to help others to classify the information. Certain documents, such as engineering drawings and customer lists, may have confidentiality marking applied as a matter of course. Employees should be invited to refer to a Trade Secret Officer or their supervisors in case of doubts.

Tip: Key considerations for setting a document marking policy

Keep document marking rules simple

Keep simple the confidentiality classification and the instructions for use of documents falling within the different categories of confidentiality. This means that only a limited number of confidentiality classification levels should be envisaged, typically no more than two or three. For example: (1) non-confidential; (2) confidential; and (3) highly confidential. Too-complex rules might be simply ignored or wrongly classified.

Apply document marking rules consistently

Inconsistent marking is misleading and can increase the risk of accidental disclosure of trade secrets by employees.

Prefer over-designation to under-designation

Instruct employees to designate documents as confidential when in doubt. In general, over-classification of information as secret should be preferred over under-classification in trade secret management. Providing employees with standard instructions to mark by default as confidential certain categories of documents could be helpful. For example, employees could be required to designate all unpublished documents containing technical details of products under development or all unpublished patent applications.

Provide clear rules on how to handle documents according to their marking

These rules should be summarized in user-friendly guidelines, easily available and accessible to employees.

Example of a document marking policy

Anika, a salesperson of Company A, collected information on client preferences for customized products. This information might be useful for the company's cross-selling activities. Company A has an interest in circulating the information internally. However, the information could be trade secret and therefore should be managed and shared carefully.

Correctly, Anika marks them as confidential. The internal "Company A's document marking policy" provides a specific discipline for documents marked as "Confidential." For example, they shall be stored separately on the data management system, in a dedicated folder that requires authorized access.

According to the policy, Anika sends an email to the Trade Secret Officer, notifying her actions, so that the Trade Secret Officer may consider whether additional actions are needed.

Regulating the creation, use and end life of documents

A significant risk to trade secret information is the accidental leakage of a document that contains it. Companies should set specific rules and adopt measures that regulate how documents (including electronic records) are handled, limiting the risks of accidental loss of control.

Example measures to regulate creation, use and end life of documents

Ban or limit copies of confidential documents, in paper or digital format.

Track unique copies of the confidential documents so that individuals can be held accountable if documents are accidentally lost. For example, create a register of unique copies listing who has received a copy of the document marked progressively, or use a watermarking system.

Oblige to store paper, prototypes, samples, etc. in safe or locked locations.

Regulate what happens to confidential documents after they have served their purpose. For example, require the recipient to return or destroy the information and provide certification of the destruction.

Manage properly the disposal of confidential documents. Confidential documents should be collected separately and securely shredded.

Regulating access to documents and information

In general, the more employees that are aware of a trade secret, the higher the chances that the company loses control over it. To reduce the risk of accidental or voluntary disclosure of trade secrets, the simplest approach is to restrict access to the trade secret and related documents. In general, access should be granted on a **need-to-know basis**, limited to the specific information and documents that are necessary for the individuals to perform their respective tasks. This principle should be applied in a balanced way so as not to unnecessarily hamper efficient knowledge sharing within the company. In a factory line, for example, a sensitive solution could be dividing a series of operations between employees so that individual employees do not know or understand the information needed for the whole process.

The company might also need to provide access to confidential documents and information to third parties. This happens frequently, considering that more and more often companies need to outsource specific activities, or collaborate on the development of new products. When there is such a need, information should be shared only as necessary. Also, access should be granted only to people or entities subject to confidentiality agreements or clauses and after obtaining approval from a person responsible for trade secret management.

Example of a "need-to-know" basis

Company A is a business consulting firm with around 500 employees. Company A has many clients. Every project is typically followed by three to five people, led by a partner. Kenzo is a partner at Company A and won a pitch for Project X.

According to the firm's policy, Kenzo opens a new folder in the data management system for Project X, the Project X Folder. At the opening of the Project X Folder, Kenzo selects the four employees of the firm who will work with him on Project X. They will be the only ones authorized to access the Project X Folder. Any subsequent request to access the Project X Folder shall be authorized by Kenzo.

All the documents and emails related to Project X shall be stored in the Project X Folder. Once Project X is completed, access to the Project X Folder is automatically disabled to Kenzo and his team.

If access to the Project X Folder is needed again, a specific and justified request must be addressed to a specific management team.

Logistics and organizational measures

The locations where companies store documents and protypes, perform research and development activities, keep servers, etc. should be supervised and access should be regulated and monitored. Logistic and organizational measures create physical barriers between a misappropriator and trade secrets.

These measures include:

- Concierge service, entry–exit registration and video surveillance at the **entrance of the company's facilities**.
- A specific **procedure applied to visitors**, including escort to the appointment area, or providing them with a name tag. Employees should be instructed to report immediately if any unknown person is located at the company's facilities.
- **Restriction on items that people can bring** into the premises, such as cameras or smartphones. In very highly sensitive areas, visitors and employees may be required to wear work uniforms with no pockets and to carry items in transparent bags.
- Badges or other automatic **identification means** to access the companies' facilities for employees.

– **Restricted access** by external visitors to the whole premises or to certain areas limited to employees only (e.g. production facilities and research and development laboratories). Access may be subject to confidentiality undertakings.

Logistics and organizational measures are usually the first point of contact with the company. Employees and visitors will recognize that the company is vigilant and ready to react if rules are broken. Therefore, it has a deterrent effect, dissuading any unlawful attempts and an educational effect on employees, encouraging the formation of a culture of confidentiality.

Education and awareness of employees

One of the most common reasons for trade secret loss is the simple accidental loss of information by those who are entrusted with trade secrets.

If employees are unaware of what a trade secret is, whether a certain piece of information is a trade secret or not, or why trade secrets are so important for the company, they could carelessly talk about them in a conversation with friends in a public place, or they could disclose information on posts and comments on social networks proudly promoting their company's (or their personal) successes.

This sort of behavior can put trade secrets in danger. To reduce such risks, the primary focus of the company should be the education of employees, with the aim to raise their awareness of the importance of trade secrets in their day-by-day work. Employees should understand that the company operates in a competitive environment, and that trade secrets are a key asset, the loss of which could be extremely harmful. Employees at all levels should be encouraged to treat trade secrets with great care in a joint effort to protect the company's competitive position.

Basic training and education of employees can generally be provided with limited costs, but with substantial effect on employees' attention to the company's trade secrets. With higher investments, it is possible to set up a more structured, continuous education program.

Implementation of internal policies, codes of conduct and codes of ethics

One way to educate employees is to provide them with a set of documents explaining how to behave, such as specific policies, codes of conduct and codes of ethics. They should serve as reminders and as a checklist for their responsibilities in the management of trade secrets, including in the remote working environment, if applicable. For example, such documents may include:

– specific rules such as a clean desk policy, a duty to return materials and documents after meetings, a duty not to store company's documents on personal devices, and a duty not to share information with third parties
– reference to local laws concerning secrecy and employees' related duties and liability.

Employees should have the opportunity to access these materials anytime (such as by posting them on the company intranet) and to ask clarifications. In addition, employees should be reminded periodically of their existence and content.

General training, tests and awards for employees

Various means exist to raise employees' awareness of trade secret management. The common goal is to engage employees and provide them with instructions and key messages.

Education should be continuous and varied. It should start with on-boarding of the employee, through an initial basic confidentiality training, and should continue throughout the employment lifecycle.

Different forms of training can be envisaged: providing employees with notices, instructional posters or videos, checklists, a list of "dos and don'ts," role play, a simulation of external threats to trade secrets such as automatically generated phishing emails, and best practice competitions with awards to individuals or teams of employees.

To create a corporate culture around trade secrets, the involvement of executives in these activities is recommended.

High-level executives and engineers should be provided with specific training that is relevant to their particular risk environment. Also, people without a direct employment relationship, such as consultants and contractors, should receive equivalent instructions.

Special training for high-risk business units

Certain functions within the company may tend to over-share sensitive information with outsiders. Usually this happens with good intentions, such as promoting the company or its products. However, this sort of behavior can be risky when trade secrets are at stake.

Here are some areas of activities that inherently have higher risks of trade secret loss, and thus special attention may be necessary:

- **Marketing activities**: people in marketing naturally like to use information about new or future products, or new features in these products, to boost promotional events or capture the interest of potential customers.
- **Business development activities**: business development activities imply similar but broader risks compared to marketing activities, since the employee is focused on new business relationships and the need to generate interest in prospective partners about the company's prospects. Here, in addition to general education regarding confidentiality, there may be a need for imposing discipline around the negotiation of, and compliance with, non-disclosure agreements.
- **Scientific publications**: in technical fields, scientists often have been trained to consider success as early publication of the results of their work in scientific journals. This inclination needs to be checked not only with basic training but with clear requirements for pre-publication submission of papers to ensure that valuable secrets are not compromised.[5]

Obviously, marketing, selling and publishing activities are all important for the business, and should be promoted and stimulated. However, proper precautions need to be taken to be sure that they are managed in a way that protects the company's trade secrets. To such end, possible measures include:

- **Provide specific training**: provide those who are involved in high-risk activities with specific training and rules to help them do their jobs with discipline and respect for the company's trade secrets.
- **Set up an approval process for external disclosures**: set up a special approval process to double-check that no sensitive information is disclosed in planned business, scientific or marketing presentations and related materials.

Information technology (IT) security measures and IT management tools

Most companies' trade secrets are stored and transmitted in globally connected digital systems that are inherently insecure. Thus, most larger companies acquire and deploy adequate IT security protections. Also, because both protective technology and risks are evolving extremely rapidly, IT security measures should be periodically reassessed.

IT security measures may include:

- **Require authentication** to access the company's IT devices, tools and systems: this may include password policy (requiring strong passwords, periodically updated), multi-factor authentication and other methods of authentication.
- Use **up-to-date** operating systems, anti-viruses, anti-spyware software, malware, firewalls.
- Implement **automatic encryption and daily back-up**.

5 See also Part VI: Trade secrets in collaborative innovation of this Guide for use of trade secrets in academic institutions for collaborative research.

- **Keep access records** for systems, folders and files, along with downloads and outgoing communications.
- Provide **specific folders** (protected by password and/or encrypted and stored in the company's system or in a secure cloud storage site) for storing confidential files.
- Set strict rules for **use and custody of electronic devices (phones, computers, tablets)** provided by the company.
- Prohibit, discourage or properly regulate the use of personal **cloud services and removable devices, possibly prohibiting the use of personal devices** (laptops, tablets, phones, thumb devices) for work-related purposes.
- Regulate the **use of the internet** as well as of devices and services connected to the internet, e.g., if appropriate and feasible, disable external connections to folders/systems that include trade secrets, issue a social media policy and ban access to certain websites.
- Have a **cyber-attack response plan** in place. The plan can include a wide range of measures, whose primary goals are stopping the attack and containing its consequences.

There are also IT tools that aim at assisting internal trade secret management. For example:

- **Software** designed to manage trade secrets. These tools (often referred to as DLP or data loss prevention) can have different functions:
  - Help companies to collect, organize, study and report their trade secrets as well as trade secrets entrusted to them by third parties.
  - Track progress in the implementation of trade secret protection measures.
  - Provide good evidence, if needed, that trade secrets are properly managed and protected, which can be useful in court to meet the "reasonable step standard" that qualifies information as a trade secret.
- **IT audits** to regularly monitor employees' activities and detect unlawful behaviors of departing employees, in compliance with local labor laws.
- **IT tools** able to provide evidence of the existence of the trade secret at specific point in time (time stamps).[6]

Part VII: Trade secrets and digital objects of this Guide contains more about security measures to protect trade secrets in digital formats as well as specific challenges and risks associated with protection of digital trade secrets.

Contractual measures

Trade secret holders should consider contractual measures for protection purposes. They can supplement the lack of other measures and are often crucial in litigation.

In drafting contracts, it is often better to refer to "confidential information" rather than to trade secrets, since the former term is more easily and broadly understood. A primary function of contracts is to define the relationship as one of confidence, and so using broader terminology reinforces that notion without predetermining what a court might find to constitute a legally protectable "trade secret."

Types of contractual measures

Types of contractual measures include confidentiality clauses and non-disclosure agreements (NDAs).

Confidentiality clauses (typically included in contracts of employment or with third parties) point out that the recipient of the information in the course of the contractual relationship shall keep such information confidential, shall not disclose to third parties and shall use it for the agreed purposes only. Confidentiality clauses may appear in any type of commercial contract, including supply agreements, sales agreements and licenses.

6 The Korean Intellectual Property Office (KIPO) launched its Trade Secret Certification Service in 2010, which received more than 188,509 cases by the end of 2022. This service takes the hash values of electronic documents and combines them with authorized time values, thereby creating time stamps. Time stamps are then registered with the Korea Institute of Patent Information (KIPI) to prove the existence of original copies of trade secrets, as well as their initial dates of possession (see https://www.kipo.go.kr/en/HtmlApp?c=91022&catmenu=ek02_06_01).

NDAs (or confidentiality agreement) are legally binding contracts that establish a confidential relationship between the parties, who agree that confidential information they may obtain within the contractual relationship will not be made available to third parties or used for purposes other than those specified in the contract. These agreements by definition contain a confidentiality clause or clauses.

Obviously, NDAs and confidentiality clauses must be properly drafted. Assistance of lawyers is advisable. Some general key considerations when drafting an NDA include the following:

- **Clearly identify which information is subject to confidentiality**. Confidentiality obligations are effective if it is clear what information is subject to confidentiality. Therefore, provide in the contract a definition of "Confidential Information," including provisions for identifying as confidential information which is communicated verbally.
- Define the **scope of rights to access, use and disclose** trade secrets, and impose **strict control measures and penalties** against breach of confidentiality by recipients.
- **Point out what is the authorized use of the information disclosed**. Specify for which specific purposes the information disclosed can be used, such as for consideration of a potential merger or license.
- **Include exceptions to confidentiality**. Clarify what is not considered confidential information, and exclude it from the scope of the confidentiality obligation. For example, information that is shown to be generally known or has entered the public domain through no fault of the recipient, or which the recipient can demonstrate was developed independently of the disclosed secrets should be excluded from the "Confidential Information" covered by the NDA.

Example of a definition of "Confidential Information" in contracts

A possible contractual definition of "Confidential Information" could be the following: "For the purpose of this Agreement, "Confidential Information" means trade practices, business plans, price lists, supplier lists, customer lists, marketing plans, financial information, software, designs, prototypes, formulas and all other information or compilations thereof which relate to [subject matter] that A will designate as confidential at the time of the disclosure to B."

In addition to confidentiality clauses and NDAs, there are contractual measures that can be used, in some jurisdictions, for the purpose of indirectly protecting trade secrets. For example, **Non-compete agreements or clauses** (also non-competition agreements and clauses) and/or **Non-solicitation agreements or clauses** may be available in some jurisdictions.

Non-compete agreements or clauses are restrictive covenants where typically one party (for example, the employee) agrees not to enter competition with the other party (for example, the employer) when they leave the company. Usually, they are limited in type of activity, geographic coverage and duration.

Non-solicitation agreements or clauses are restrictive covenants where typically one party (for example, the employee) agrees to be prohibited from diverting the company's clients or recruiting its employees upon leaving the company. Their allowability varies from one jurisdiction to another. These agreements that are typically concluded between an employer and its employee will be addressed further in the next section.

Although acquiring information through reverse engineering is generally considered as not constituting misappropriation of trade secrets, many countries, such as most Member States of the European Union, do not prohibit trade secret holders to enter into a **contractual agreement that prohibits reverse engineering**. In general, the United States of America enforces anti-reverse engineering clauses in contracts between business entities. The extent to which contractual clauses can prevent reverse engineering also varies among national laws.

Contracts with employees

Depending on national approaches, the law or the contract may imply that the person receiving the trade secret cannot use it, except for the uses agreed between the parties, and must maintain confidentiality. This is true at least for employees, since an obligation not to disclose the employer's trade secrets is generally implied in the duty of loyalty and fidelity of the employee.

Despite legal confidentiality obligations, providing (additional) **contractual confidentiality obligations**is highly advisable, at least for the following reasons:

- **NDAs and confidentiality clauses provide more certainty**, compared to implicit obligations stemming directly from the law, which vary among countries.
- **NDAs and confidentiality clauses have additional effects against trade secrets misappropriation from employees and third parties**. Companies that ask their employees to sign NDAs send a clear message that the company cares about its trade secrets. Actively signing NDAs may create deterrent to breach of confidentiality obligations.
- **NDAs and confidentiality clauses generally make enforcement easier**. The trade secret holder could often raise in court a contractual claim and a non-contractual claim based on the national/regional trade secret laws. The two claims will likely overlap to some extent, but depending on the national approaches, there could be differences in terms of burden of proof, remedies, and statutes of limitation. Having two shots raises the chances to hit the target. In addition, courts are more likely to find liability when confidentiality obligations are clearly set forth in a contract.

Including confidentiality clauses in employment agreements is recommended. To be on the safe side, it is highly advisable to always specify in the contract of employment that **confidentiality obligations last beyond the termination of the contract of employment**, and check if such clause is admissible under the applicable law.

Non-compete agreements restricting the possibility of the employee to compete with the employer contain a more pervasive contractual restriction than confidentiality clauses or NDAs.

There are generally no issues when the non-compete agreement refers to the period when the employment is in force. **The enforceability of the non-compete agreement after the termination of the employment, however, requires attention** due to its wide-ranging effects. A non-compete agreement may prevent employees from using not only trade secrets, but also their general knowledge, skills and experience, conflicting with the mobility of workers.

Accordingly, some countries prohibit non-compete agreements, save in exceptional circumstances. If not forbidden, non-compete agreements are nonetheless generally subject to certain limitations and boundaries. They typically must be "reasonable" in geographic coverage, duration and scope. A non-compete agreement lasting one or two years, covering the geographic area and the kind of work performed by the employee in his or her previous employment is generally acceptable in several countries.

Considering the many variations in national approaches[7] regarding non-compete clauses/non-compete agreements, companies (in particular, multinational companies) should pay attention to drafting such clauses. Employers should also consider the possible counter effects of including non-compete agreements in their employment contracts of employment, as they may be perceived as unfair by employees, lower their morale or discourage job applications.

NDAs, non-compete agreements and/or confidentiality clause should **be signed at the very beginning of the relationship** between the parties before any exchange of confidential information. Remedying their absence at a later stage is possible, pointing out that the confidentiality obligations undertaken by the parties apply also to information

7 For a country-by-country overview of post-termination of employment restrictions, see, for example, Confidential Information, Trade Secrets and Post-Termination Restrictions, 2023, Bird & Bird. https://www.twobirds.com/en/insights/2023/global/global-guide-on-confidential-information.

exchanged previously. However, the risk of discussing confidentiality obligations ex post is that disagreements could emerge on the terms of the agreement, while confidential information has already been exchanged. In such a situation, the party who disclosed a trade secret or confidential information would not have much contractual power to impose its preferred conditions.

Contracts with third parties[8]

In the modern economy trade secret holders may need to share their trade secret information with third parties for, for instance, collaborative research, joint venture activities, manufacturing or distribution arrangements, franchising, fundraising etc. To achieve a specific business need, trade secret information may be shared with external consultants, contractors, vendors, distributors, sales agents, commercial and technical partners, and also potential business partners. These relationships are of temporary nature, and the third parties may have worked, be working, or work in the future, with competitors. Therefore, the need to protect confidentiality can be greater with third parties than employees. Trade secrets must be particularly protected toward **third parties, with whom the trade secret holder cooperates**.

It is recommended to **include by default confidentiality clauses** in all contracts entered into with third parties. Alternatively, signing a separate NDA focusing on confidentiality and exchange of confidential information is advisable when: (i) the exchange of confidential information is needed before the signing of the contract, for example, to draft it properly; (ii) the regulation of the exchange of confidential information is more complex and deserves to be addressed separately in more detail; (iii) the contractual relationship between the parties is already established in a contract that does not include a confidentiality clause, or (iv) the disclosing party needs to disclose a highly valuable trade secret that deserves additional commitments.

If a trade secret holder discloses their trade secret information to, for instance, a consultant who will use that information to deliver its service, the contract should specify that the consultant shall not use the disclosed trade secret information for any other purpose. In addition, the trade secret holder must make sure that the consultant will not use trade secret information of any other person for performing the contracted work (see Section 5.2).

The **general advice regarding contractual measures** (see Section 2.3 above) **also applies** to confidentiality clauses and NDAs with third parties. For example, NDAs should be signed, and contractual clauses should be introduced, in the beginning of the working relationship, and if applicable, non-compete agreements may be set-up. In particular, they should point out:

- **what** kinds of information are protected
- **how** they are protected
- what are the **restrictions on their access and use**
- if applicable, how and to what extent the recipient is authorized to **share them with other third parties**
- what is the **duration** of the confidentiality obligation, and any **obligation after the termination** of the contract, and
- what happens to the **confidential documents when the collaboration terminates**.

8 See Part VI: Trade Secrets in Collaborative Innovation) of the Guide, in particular, Section 2 on use of NDAs and confidentiality clauses in collaborative activities.

Case example: "The Serve Machine 1100" – Step 3

The Super Tennis Racket Company analyzes the risk assessment report concerning "The Serve Machine 1100" and decides to take the following measures.

Measures against risk 1 – potential leakage

- Specific employees will be assigned to "The Serve Machine 1100," and these employees only will be authorized to access the dedicated area.
- Access to the dedicated area will be possible only through automatic doors that can be opened by swiping the authorized employees' personnel badges.
- The entrance to the dedicated area will be controlled by a video-surveillance system.

Measures against risk 2 – potential misappropriation (measures applicable also to mitigaterisk 1)

- The legal department will send a communication to all employees reminding them of their confidentiality obligations included in their contracts of employment.
- The legal department will provide basic training to all employees on the importance of the company's information assets, as well as the need for preserving them and for all employees to play their part.
- All employees assigned to "The Serve Machine 1100" will receive specific training on the importance of the secrecy of "The Serve Machine 1100" and will be required to sign specific NDAs.
- The team that developed the "The Serve Machine 1100" will receive specific training on the importance of maintaining the secrecy of their work at the R&D department. Also, they will be trained on the risks of being targeted by competitors to access the company's trade secrets, and will be required to sign specific NDAs on their activities.

Measures against risk 3 – potential contamination

- Louise carried out further investigations. While the IT team checked Caspar's activities on his computer, nothing suspicious emerged. Caspar has never uploaded external documents of dubious origins on The Super Tennis Racket Company's data management system.
- Louise talks with Caspar to better understand the situation. Caspar assures her that he had not misappropriated any trade secrets or confidential documents from his previous employers. He also assures her that, while employed at The Third Set, he had never worked on anything similar to "The Serve Machine 1100."
- The research and development team that worked on the development of "The Serve Machine 1100" will collect all the documents that can be used to show the independent development of the machinery, to be ready to react to any misappropriation claim from The Third Set or other competitors.

2.4 Step 4: Monitor and react to misappropriation and leakages

Trade secret protection plan (Step 4)

General principles for an efficient reaction

Even with a strong and efficient trade secret protection plan and a careful trade secret management policy in place, misappropriation of trade secrets can occur. In general , trade secret misappropriation means acquisition, use or disclosure of trade secrets through unlawful, improper, or dishonest means (see Part III: Basics of trade secret protection of this Guide).

Also, accidental disclosure by, or leakages from, the trade secret holder may also happen, due to negligence or a simple mistake. For example, accidental disclosure can occur when a confidential document is mistakenly sent via email to the wrong recipient.

Three important general principles should be kept in mind for an efficient reaction to leakages and misappropriations.

1. **Do not get emotional**: reactions to leakages and misappropriation of trade secrets should be considered as an integral part of trade secret management, which is largely based on risk management. The important thing is to be ready and prepared to react, avoid further damages, counterattack at the right time and recover.
2. **Consider that speed of reaction is crucial**: a good reaction can be useless if it comes too late. One of the major risks of misappropriation or leakages is that the trade secret is publicly disclosed and loses its entire value. A timely reaction may prevent further disclosure or misuse, or at least limit its negative consequences.
3. **Have a response plan ready**: a response plan should be in place before the incident occurs. Appoint one or more persons responsible to take actions in the emergency. Everyone in the company should be instructed to report immediately any threat to trade secrets.

In general, trade secret holders may take the following steps to react to misappropriation or leakages.

- Understand the situation and stop the misappropriation or leakage
- Preserve the trade secret value
- Cure the reason for the breach
- Handle the reputational damage and liability

These typical steps that are taken within the trade secret holder's organization will be detailed, below.

Understand the situation and stop the misappropriation or leakage

To avoid deleterious power vacuums and blame-shifting when the misappropriation occurs, the trade secret management policy should provide initial indications and guidance to those who are in charge of handling the situation.

In general, there are three initial steps that should be taken, both in terms of trade secret management and potential trade secret litigation.

1. **Collect and preserve evidence** of the possible trade secret misappropriation or leakage. It is good to have as many options as possible for reacting at a later stage. For example, while the trade secret holder may decide, in the beginning, to pursue an out-of-court solution by sending a warning letter, if the alleged misappropriator does not react, the trade secret holder could decide to move to litigation, if evidence of misappropriation is well preserved.
2. **Investigate** what happened. In particular, understand how the misappropriation was possible and who carried it out. Obviously, investigations should be carried out in a confidential manner so as not to alert the alleged misappropriator, who could take countermeasures or destroy evidence.
3. **Detect the weaknesses** that caused the misappropriation/leakage. If needed, take emergency measures to **mitigate immediate harms** and **avoid further violations**. A comprehensive and detailed review of the trade secret protection plan will be possible at a later stage.

Obviously, the three steps above could interrelate with each other. For example, preserving the evidence likely implies a first initial understanding of the situation. However, waiting too long before taking action bears the risk that evidence could be lost or altered.

Preserve the trade secret value

After adopting evidence preservation measures, understanding what happened, and taking an initial step to prevent further unlawful acquisition and/or use of the trade secret, the company has to decide how to react to the misappropriation.

The company should not lose its focus on the ultimate goal of trade secret management: the maximization of the benefits of the trade secrets to gain and sustain a competitive advantage. This goal does not change because of the leakage or the misappropriation. What changes, however, may be the way to achieve it.

If the leaked trade secrets have not yet been made public, the holder could consider the following options:

- **Amicable resolution**: get in contact with the misappropriator to agree on immediate return/destruction of any physical materials carrying the trade secret information, stop using and disseminating the trade secret information and settle any possible dispute. This could satisfy the goal to quickly stop the dissemination or misuse of the information
- Seeking an amicable solution could be a good option to consider for business and commercial reasons. In cases where the parties cannot quickly resolve the dispute, they may be able to agree on a mediator to help them find an amicable solution.
- **Litigation**: immediately start litigation, also with the purpose of obtaining a preliminary injunction from the competent courts to enjoin and prevent further violations (see Part V of this Guide (Trade secrets in litigation) for court remedies in litigation). Litigation, however, often leads to a settlement of the dispute between the parties.

If the **misappropriated trade secrets have already been made public**, the trade secret holder has lost legal protection for the information. In this scenario, one option is to **start litigation** to obtain damages, if the other party is not willing to compensate the harm voluntarily. However, there are other possibilities to settle the dispute, such as **establishing an amicable business relationship** as a licensing partner, a distributor, a business partner or an external consultant, which can be used as a means to provide compensation.

Cure the reason for the breach

After the incident, review the trade secret protection plan and its implementation, and identify its potential weaknesses. If needed, amend or improve the protection plan to avoid any similar episode in the future. The reason for the breach can be identified with different means, e.g., internal due diligence, software designed to manage and protect trade secrets, or "stress tests" of the IT system.

Consider whether it is appropriate to start disciplinary actions against employees, or contractual action against third parties, who are responsible for the trade secret leakage or misappropriation. The incident can also be an opportunity to educate and train employees: for example, the lessons learned and areas for improvement to avoid such incident in the future.

Handle the reputational damage and liability

Trade secret misappropriation can give rise to contractual and tort liability. This is the case where, for example, leakage of a trade secret occurred because a licensee of the trade secret under the confidentiality obligation disclosed it. In addition, a misappropriation could give rise to a duty of communication towards clients, suppliers and public authorities. Legal professionals may provide appropriate advice in these situations.

Suffering a misappropriation/leakage of its trade secrets can negatively **impact the reputation of the company, its goodwill and public perception**. Taking advantage of the situation, competitors may emphasize the inability of the company to protect its trade secrets or those of its partners or customers. Therefore, **quickly setting up a communication campaign**, targeted to the general public or limited to certain entities, authorities, clients or commercial partners as well as to employees, can be important. A PR communication could be a good way to start to rebuild your reputation, letting the market know that you care about trade secrets, and how

significantly you improved the management and protection of confidential information after the incident.

In some countries,**insurance products** to mitigate the risks relating to trade secret misappropriation and leakages are available.

Case example: "The Serve Machine 1100" – Step 4

It took some time and effort, but The Super Tennis Racket Company has finally implemented all the measures it had identified as reasonable to protect the features, design and specifications of "The Serve Machine 1100."

Louise is now on vacation. She scrolls the home page of her social network account and while scrolling, she sees that Kai, a worker assigned to "The Serve Machine 1100," posted a picture on his social network account. In the picture, there is Kai with a couple of colleagues to celebrate the birthday of one of them. In the background, there is "The Serve Machine 1100."

Louise reports the incidence immediately to the "Report TS threats" email. Kai is quickly contacted and asked to remove the picture.

Following the internal investigation, the company takes the following actions:

1. The picture was taken in the room dedicated to the "The Serve Machine 1100," and all the employees in the picture were authorized to be there.
2. Luckily, the research and development team assures that no relevant details of "The Serve Machine 1100" can be seen in the picture. The picture did not disclose any secret information. The trade secret is still a secret.
3. To avoid similar episodes in the future, management decides to introduce a no-phone rule in the room dedicated to "The Serve Machine 1100."
4. The management sends a serious email to Kai, reminding him of his confidentiality obligation, the severe breach of the policy that he committed and the risk that the company faced because of his negligent conduct. However, the company decided not to take other actions against Kai, considering that, in the end, the company suffered no damages.

The management sends another email to the whole company, explaining what happened, including the negative impact that this episode could have had on the company. The new no-phone rule in the room dedicated to "The Serve Machine 1100" is notified to all the employees. The management also stresses that more severe actions will be taken if something similar should ever happen again.

2.5 Sample checklist: Trade secret management plan

This section provides an outline of four steps detailed in Sections 2.1 to 2.4 in the form of a sample checklist. It may be used by businesses to help in setting up a trade secret management plan to identify and protect trade secrets against misappropriation and leakage. However, it is neither an exhaustive list nor a boilerplate list that must be implemented by all readers. The sample checklist should be adapted to the specific needs of each business, depending on, for example, their size, resources, business sector and market environment.

Sample checklist A: Implementation of a trade secret protection plan against misappropriation and leakage - what steps to take

1. Identify and value your "potential" trade secrets

Identify the company's valuable information. Consider the following steps:

✓ interview key employees and managers
✓ analyze data on production, sales, customer satisfaction
✓ analyze competitors' products and customer preferences to understand which product features drive success in the market.

Select important trade secrets. Usually, only a subset of the information collected under the sub-step above is worth implementing special protection measures. In case of doubt, prefer a broader selection of information than a narrower one.

Create a catalogue of the trade secrets, using high level descriptions.

2. Identify the risks for your trade secrets

Identify the potential risks for your trade secrets. Consider the following major risks:

✓ third parties' acquisition of the trade secret
✓ leakages and accidental disclosures of the trade secret from the holder or third parties entrusted with the trade secret
✓ third parties claim that you misappropriated their trade secrets.

Determine the potential impact (severity of the consequences).

Produce a risk assessment report identifying potential risks, likelihood of occurrence and their consequences, as a basis to prioritize the interventions needed.

3. Identify and apply reasonable protection measures

Decide what are the reasonable secrecy measures to apply. Consider the following factors:

✓ the characteristics of the organization (the size, resources etc.)
✓ the peculiarities of the business sector (e.g., nature and extent of risk of leakage, loss of control or contamination) and the effectiveness of particular measures in that sector
✓ the costs (in terms of money and efficiency) of particular trade secret protection measures.

Having identified the reasonable secrecy measures to the relevant trade secrets, consider implementing the operational and contractual measures.

3.a Implement operational measures

Set up clear trade secret management roles and decision-making processes:

✓ establish clear roles and responsibilities for taking trade secret management decisions
✓ clarify and streamline the trade secret management decision-making process
✓ appoint a "Trade Secret Officer"
✓ set up an emergency plan in place for critical situations that might arise.

Set up document management measures:

✓ apply a document marking policy
✓ regulate the creation, use and end life of documents:
  – ban or limit copiestrack unique copies for the most sensitive documents
  – require storage of confidential material in safe and locked locations
  – regulate what happens to documents containing confidential information after they have served their purpose
  – manage properly the disposal of confidential documents.

Implement logistics and organizational measures:

✓ create physical access barriers, for example:
  – measures at the entrance of the company's facilities
  – a specific procedure for visitors
  – restriction of items that people can bring into the premises
  – badges and other identification means
  – restricted access to the whole or limited areas by external visitors.

3.b Education and awareness of employees

Implement internal policies, codes of conduct, codes of ethics.

Create a corporate culture around trade secret by providing general trainings, tests and awards to employees.

Provide specific trainings and supervision to people involved in high-risk business units.

3.c Implement information technology (IT) security measures

IT security measures may include:

✓ require authentication to access the company's IT devices and systems
✓ use up-to-date software, automatic encryption, daily back-up etc.
✓ keep access records for systems, folders etc.
✓ provide specific folders for storing confidential information
✓ set rules for use and custody of company's IT devices
✓ regulate the use of cloud services and removable devices
✓ regulate the use of the internet
✓ have a cyber-attack response plan in place
✓ as appropriate, consider IT tools that aim to assist trade secret management.

3.d Implement contractual measures

With entities inside the company:

✓ require employees to undertake confidentiality obligations, in the form of confidentiality clauses or non-disclosure agreements
✓ require employees having access to strategic information to sign specific non-disclosure agreements and, if appropriate and possible, non-compete and/or non-solicitation agreements.

With entities outside the company:

✓ require suppliers, customers and commercial or technical partners to undertake confidentiality obligations, in the form of confidentiality clauses or non-disclosure agreements.

4. Monitor and react to misappropriation and leakages

Understand the situation and stop the misappropriation by:

✓ collecting and preserving relevant evidenceinvestigating what happened
✓ detecting the weaknesses that caused the problem, mitigating immediate harms and avoiding further violations.

Consider how to deal with the source of the problem, e.g., seek amicable resolution or litigation.

Review the trade secret protection plan and its implementation, improving it to avoid future incidents.

Handle reputational damage and liability by:

- ✓ considering any contractual and tort liability considering any duty of communication towards clients, suppliers and public authorities
- ✓ mitigating any negative impact on the reputation, goodwill and public perception of the company by, e.g., a communication campaign.

3. Situations with a high risk of misappropriation

3.1 Exit of employees and risks of misappropriation[9]

Leakage of trade secrets can occur through different channels, such as from current employees, former employees and retirees, external contractors, hackers etc., however, it is well known that trade secret leakage by employees changing jobs is one of the high-risk situations that many companies confront.

Usually, employers and departing employees have **conflicting interests**. Former employers may want to prevent their employees from passing on the knowledge acquired through their former employment to new employers. Employees, however, may want to advance their career at the new employer, or start their own business, based on what they have learned at their former employers. New employers do not want to get into trade secret misappropriation disputes with the former employers due to the recruitment of new employees and also wish to prevent contamination of their own information assets (see Section 5 regarding contamination with former employers' trade secrets).

Trade secret law, labor law and antitrust law etc. are the legal instruments that aim at balancing these various interests. Confidentiality clauses, non-disclosure, non-compete and non-solicitation agreements are also typical legal tools that may be used to mitigate the risks of disputes stemming from employees' mobility (see Section 2.3). However, to what extent the former employers can prohibit the employees' job mobility and the use of their knowledge after the job exit, and to what extent the employees have the freedom to choose a new job and use their knowledge,**vary significantly among jurisdictions**. Also, this depends on the circumstances of each case.

Therefore, assistance from experts who are familiar with the applicable law is indispensable. Broadly speaking, information that is general knowledge and skill of the employee is not a trade secret that can be claimed by the former employer.

While contractual measures, together with training and educational programs about trade secret protection, may have a deterrent effect for preventing potential disputes over misappropriation of former employers' trade secrets, there are also additional measures, some of which should be taken before the employee leaves the company, while others should be taken after the employee has left the company.

Measures to take before an employee's exit

Where an employee submits their resignation, several measures can be taken to mitigate the risks of misappropriation.

First, depending on the circumstances of the case, consider foreclosing **the employee's access to trade secrets and confidential information** as soon as the employee communicates his or her resignation. The company should make a risk assessment, considering various issues case by case, such as: (i) the need to continue the projects being managed by the employee; (ii) the

9 The outline of measures that may be taken in situations with a high risk of misappropriation is found in Section 3.3 below.

costs of keeping the employee on the payroll; and (iii) the risks run by letting the employee have access to the information asset of the company until their last day of work.

In addition, the departing employees should be reminded of their obligation to **return or destroy** any confidential documents or other materials. Such obligation should be found in the confidentiality clauses of employment contracts.

Exit interviews are also an important action to mitigate the risk related to employees leaving the company. Whether employees resign or they are let go by the employer, schedule exit interviews to **remind employees of their legal confidentiality duties** and their specific **contractual obligations**. Information regarding **the departing employees' reasons for resignation** and the **employees' new job** generally provide the degree of caution required by the company.

Exit interviews can have an important psychological and deterrent effect. The departing employees will perceive and remember that the company cares about its trade secrets and it is ready to react to protect them, if forced to do so. Therefore, the risk of misappropriation or misuse of the employer's trade secrets likely decreases. Exit interviews are low-cost measures that can help the trade secret holder to demonstrate to a court that it had taken "reasonable steps" to keep the information secret.

To identify any leak as quickly as possible and stop any further dissemination or unauthorized use of the trade secret, companies generally **check the IT devices**, tools and systems used by employees leaving the company to identify any anomaly in their behavior. Usually, the period between the notice of termination and the last several days of work is critical, as departing employees may download files from their devices and systems, send them to personal email addresses, upload them on personal cloud accounts, or simply print or collect them in hard copies. Since scrutinizing employees' activities is a delicate operation that must be done in compliance with the applicable labor law, privacy rules and IT forensics best practices, the assistance of (external) experts is recommended.

Reducing turnover of employees is another way of mitigating risk. Establishing a good working environment through, for example, investments in employees' welfare, promotion of better work–life balance and communication between management and employees, may have a positive effect on the retention of employees.

Measures to take after an employee's exit

Following the termination of employment, consider possible measures aimed at keeping the departing employees aware of to their obligations.

For instance, depending on the circumstances, if there are high concerns of misappropriation related to the new employment, it may be appropriate for the former employer to **send a communication to the departing employee and/or to the new employer**. Once such a communication is received, the former employee and the hiring employer will likely adopt a higher level of caution, as they will be unable to claim that they were not aware of the trade secrets. These communications should be sent with great care and drafted with the assistance of a lawyer, because they could be perceived as, or actually amount to, defamation or retaliation under applicable national laws.

Also, in the post-employment period, it is important to be **attentive to "signals"** that may indicate potential risk of trade secret misappropriation and require further investigation. For example, it is advisable to monitor the activities of the competitor who hired the former employee or the activities of the business that the former employee set up after their resignation. If the competitor releases, shortly after the joining of the new employee, a new product having features that can be achieved only by using the secret process developed by the former employer or files a patent application that claims an invention deriving from the trade secrets, this should reasonably raise serious concerns.

In addition, keep an eye on whether **other employees depart in the same period**. If they all join the same competitor, particular care is needed. The competitor could have targeted a

specific work group inside the trade secret holder's organization to recreate it within its own company (so called "poaching of employees"), therefore trying to also appropriate the former employer's know-how.

Reaction to misappropriation carried out by a former employee

If a former employee downloaded a large amount of the company's confidential documents before moving to a competitor and the competitor releases, shortly thereafter, a new product based on the technology protected by trade secrets, it may justify a strong inference of trade secret misappropriation by the former employee.

In reality, however, whether improper dissemination of trade secret information by the former employee has actually occurred is often ambiguous, and the former employer has a good reason to be concerned about the risk of misappropriation of trade secret information carried in the head of the former employee.

Therefore, determining misappropriation by former employees is a complex question that requires special investigation, assessment of circumstantial evidence and tactical consideration.

Having said this, the general rules concerning reaction to misappropriation (see Section 2.4) can be adapted to the specific exit of employee scenario as well.

- **Do not get emotional**: the previous co-worker relationship with the former employee usually heightens emotional reactions when a suspicion of trade secret misappropriation arises. Stay calm and stick to your trade secret protection plan.
- **Collect and preserve evidence**: if possible, freeze the evidence of the misappropriation or the leakage. This usually needs the involvement of technical forensics experts and legal counsel.
- **Investigate the situation and collect information**: investigation and collection of information should be carried out with great care to avoid destruction of evidence, such as metadata related to specific records. For a better understanding of the situation and/or to limit any negative consequences, one possible course of action is to seek the former employee's explanation about their behavior and demand their cooperation to limit the damage. However, this might not be the best option, if the strategy of the employer is, for example, to file litigation and seek preliminary injunction and seizure orders against the new employer of the former employee (see Part V: Trade secrets in litigation of this Guide).
- **Preserve the trade secret value**: consider whether to take any legal action against the former employee, taking into account the seriousness of the violation. Amicable resolution with the former employee and/or their new employer should be an alternative way of settling the case.

After the initial actions, the trade secret protection plan should be **critically reviewed to identify any weaknesses** that caused the misappropriation. For example, inclusion of stronger confidentiality clauses in employment contracts, introduction of (higher) penalties in case of breach, and improvement of education and awareness of employees or introduction of stricter access restrictions to documents and information.

In general, if an employee or a former employee is involved in trade secret misappropriation, your reaction may have an **impact on other employees' behaviors**. You need to send a clear message: the company cares about trade secrets and violations of the company's rights will not go unpunished.

Case example: "The Serve Machine 1100" – the disloyal employee

The Super Tennis Racket Company implemented all the measures it had planned to protect its "The Serve Machine 1100." "The Serve Machine 1100" becomes a key asset of the company. The company knows it and protects it diligently.

One day, bad news arrives: their competitor, The Bad Player, has hired Anna, a member of the research and development team that developed "The Serve Machine 1100." At her

exit interview, Anna had said that she was leaving to help her mother on the family's farm. However, after Anna's departure, The Super Tennis Racket Company learns from several people that she had started a new position at The Bad Player.

Louise is not worried. The company knew this could have happened. It was a calculated risk, and the company knows exactly what to do.

Louise and The Super Tennis Racket Company react as follows:

In accordance with the trade secret protection plan of The Super Tennis Racket Company, the IT team had checked the company's devices used by Anna at the time of her exit and found nothing suspicious. No confidential documents have been downloaded. However, Louise asks the IT team to carry out a deeper analysis. It comes out that during the last few days before her departure, Anna opened an impressive number of documents, just for a few seconds each, on her business laptop. Many of them concerned the "The Serve Machine 1100" and there was no work-related reason for her to open them, since she was working on other projects at the time.

After some internal investigation, Louise finds out that Hester, a colleague of Anna, entered Anna's room to say goodbye to Anna on her last day. Hester found Anna taking pictures of the laptop screen with her personal smartphone. Anna appeared clearly uncomfortable and said that she was taking pictures of some personal photos left on the laptop. Clearly, Anna must have opened the documents concerning "The Serve Machine 1100" to take videos or pictures with her smartphone.

The Super Tennis Racket Company hires an external computer forensics expert and asks them to freeze the evidence of the operations carried out by Anna in the last days of work at The Super Tennis Racket Company. This is good evidence that can be filed in court.

The Super Tennis Racket Company is ready for the counterattack. The company files a lawsuit against The Bad Player and Anna for trade secret misappropriation. The Super Tennis Racket Company asks the Court to take urgent measures to: (i) inspect Anna's electronic devices and The Bad Player's data management system to detect The Super Tennis Racket Company's trade secret information and documents; and (ii) prohibit Anna and The Bad Player from using the misappropriated trade secrets and documents.

The Super Tennis Racket Company obtains and enforces the court order. The Bad Player and Anna did not expect such a prompt reaction. The Super Tennis Racket Company's documents are found on Anna's smartphone and The Bad Player's data management system. The Court further orders the destruction of the misappropriated documents and prohibits both Anna and The Bad Player from using the misappropriated information.

The trade secret is safe (the secrecy of the valuable information is still intact), and The Super Tennis Racket Company can continue to enjoy the commercial benefit derived from the trade secret information relating to "The Serve Machine 1100."

The Super Tennis Racket Company releases a public statement. The Super Tennis Racket Company was a victim of a trade secret misappropriation attempt. However, the trade secret protection plan set up by the company worked efficiently and the company knew what to do. The threat was neutralized. Competitors and employees are warned. The Super Tennis Racket Company knows how to protect its trade secrets.

3.2 Risk of misappropriation when trade secrets are shared with external parties

A critical risk for trade secret holders arises when they share their confidential information with other parties outside the organization. Sharing of trade secrets with others may be necessary when, for example, conducting collaborative research or manufacturing with another organization, or outsource specific activities to another organization.

Since Part VI of this Guide focuses on trade secret-related issues in collaborative innovation, including handling of each party's trade secrets that are brought into collaborative innovation and trade secrets that are generated through the collaborative activities, this section merely highlights several general issues that trade secret holders should consider when sharing their trade secrets with others.

Best practices for trade secret holders

For **trade secret holders**, they should be particularly mindful of the following general best practice.

Carefully choose your partner. It is important to select properly your potential partners. They have to be trustworthy. Signing a contract does not assure you that the other party will duly perform its obligations. You can certainly file a breach of contract action in court, but compensation for damages could hardly fully restore your loss. This is particularly true if the trade secret has been disclosed to the public, resulting in the loss of legal protection. In addition, obtaining damages generally requires long and expensive litigation. Therefore, the first golden rule is **to know well and have trust in your partners** before disclosing your trade secret information to them.

Use NDAs and enter into solid contracts. Enter into an NDA with potential partners (including customers and suppliers) at the very beginning of the business relationship, i.e., when starting negotiations. For trade secret holders, it is preferable to oblige the recipient to observe confidentiality permanently.

Once you have chosen a good partner, sign a good contract. Contracts can be a very important tool to regulate collaboration with other parties. See Section 2.3 with respect to confidentiality clauses in contracts with third parties and NDAs.

Carefully share your information and monitor its use. At the end of the collaboration, the recipient party should be **reminded of its confidentiality obligations and the ownership of** the respective information. Ask the recipient to **return or destroy** confidential documents in its hands and to certify such destruction.

Provide the recipient party **only with the information that is strictly necessary** to perform its tasks. You may also **monitor the work of the recipient** and its use of the information that has been shared. During the collaboration, mark any document shared as confidential and use wording that identifies the trade secret holder. In addition, secured databases that track accesses to shared documents may be used instead of emails.

Require recipients to adopt high standards of protection. Require the recipient party to adopt **at least the same standard of protection** you would apply to protect your own trade secrets. Preferably, if there are specific steps that you believe could provide more reliable and predictable protection, require the recipient to follow those steps.

Carefully define the rights of each party in any newly created work. When a trade secret holder shares the confidential information with another party who uses that information for creating something else (e.g., a new invention), it is very important that both parties agree, in advance, **who has legal control over the shared trade secret** and who has **the rights in the newly created work**.

Similarly, a party who receives the information might make improvements or modifications to it. Typically, trade secret holders try to negotiate owning such information as improved or modified by the recipient.

Periodical review and update. Since business relationships can change with time, review the obligations in agreements with third parties, and update them, as necessary.

Turning to the recipient of trade secret information, **receiving such information from the trade secret holder comes with the obligation** to properly protect, use, and manage it in accordance with the terms and conditions of the contract and the law. This is not a light responsibility, since these contracts usually stipulate the liability of the recipient party if it does not fulfill its obligations contained in the contract or mismanages the trade secrets received. In particular, trade secret holders usually allow recipients to use the trade secret information only for a certain purpose. Therefore, the recipient companies should make sure that their employees who are exposed to that secret information will **not use it for other purposes**. In addition, the recipient should take reasonable steps to keep the information secret.

Consequently, a comprehensive trade secret management strategy covers proper management of trade secrets that are generated by the company as well as trade secrets of another company that the company is authorized to use.

If you are authorized to use trade secrets of a third party, to reduce the risk of mismanagement of the third party's trade secrets:

- **identify** your right and obligation regarding the use of the trade secrets and the standard of protection to maintain the secrecy of the trade secret information
- **monitor** compliance with the obligation stipulated in the contract
- **store confidential documents and information of the third party separately** from your company's trade secrets to avoid contamination (see Section 4, below, on preventing contamination by trade secrets held by others).

3.3 Sample checklist: Departure of employees and sharing trade secrets with other parties

The following sample checklist summarizes the measures that can be helpful for reducing the risk of misappropriation and leakage of trade secrets in two specific situations described in Sections 3.1 and 3.2, namely, departure of employees and sharing trade secrets with external parties. As indicated in Section 2.5, it should be used as a sample that requires adaptation to the specific needs of each reader.

Sample checklist B: Situations with high risk of misappropriation – Examples of measures

Departure of employees

Before the employees' departure

1. Assess the risk of allowing departing employees to access trade secrets until the last day of their work
2. Schedule exit interviews to:
   - remind employees of their legal and contractual obligations of confidentiality
   - ask about the employees' new job and their ability to comply with their confidentiality obligation
3. Consider checking the company's IT devices and systems used by the employees (beware of applicable privacy and other laws)
4. Remind the employees to return any documents or other materials that contain confidential information (enforce the relevant contract clauses)
5. Implement measures that reduce the turnover of employees

After the departure of employees

1. Consider, if appropriate, sending a communication to the departed employees and/or their new employers, flagging the need to respect the former employer's trade secrets
2. Monitor the activities of the new employers or of the business set up by the

former employees
3. Monitor whether other employees depart in the same period. Pay particular attention if they all join the same competitor

Sharing information with other parties and joint cooperations

For trade secret holders

1. Choose a contractual party that is trustworthy
2. Use non-disclosure agreements with potential partners when starting the negotiations
3. Enter solid contracts with confidentiality clauses. For example:
   - require the recipients to adopt a high standard of protection
   - carefully define the rights of each party in the newly created work
4. Carefully share your information and monitor its use. For example:
   - share only information that is strictly necessary to perform the agreed tasks
   - monitor the work of the recipients and their use of the shared information
   - mark shared documents as confidential
   - use protected databases that track access to shared trade secret information, instead of using emails
5. At the end of the collaboration, remind the other party of its confidentiality obligations and who owns particular information
6. Remind the recipient to return or destroy confidential documents in its hands and to certify such destruction (enforce the relevant contract clauses)

For the recipients of others' trade secrets

1. Identify your rights and obligations
2. Monitor compliance with limitations on authorized use
3. Store any received confidential information separately from your trade secrets

---

4. How to avoid contamination with third parties' trade secrets

4.1 The paths of contamination

In addition to reducing the outbound risk of leakage and misappropriation of its own trade secrets, the trade secret holder should also address how to avoid the inbound risk of contamination with others' trade secrets.

Contamination means **receiving others' trade secrets that you did not want, or you did not expect to receive**. The previous Section discussed how to protect trade secrets as internal assets of the company from external leakages and misappropriation from external parties. In this Section, we address how to protect the company's internal information assets from the potential taint of third parties' trade secrets.

Contamination could occur, for example, when Company A transmits to Company B its trade secrets, willfully or accidentally, while Company B is not interested in receiving this information. Contamination with third parties' trade secrets could also be the result of a chain of dissemination of trade secrets through more than one party. Once the information finds its way into the company, it can spread very quickly and widely. The information might be used within the company in multiple projects, re-elaborated or incorporated in some new products, transferred to someone else, taken as an inspiration or used as a basis for a new business plan or a marketing campaign.

Third parties' trade secrets may enter a company through different paths. In particular:

- Through **new employees**: frequently, contamination occurs because new employees who take information and documents of the former employer use them to perform their duties in the new job, without any knowledge of the new employer.

- Through lawfully **acquiring trade secret information of another party**: contamination may occur when a company is engaged in a business transaction with another party where the latter's trade secrets are shared during, for example, licensing or merger negotiation.
- Through competitive intelligence: contamination could occur when a company gathers business information of competitors (competitive intelligence).[10]

Frequently, people interact with others in the same business sector, receive marketing proposals, discuss business offers and negotiate agreements, sharing a great deal of information in the process. Thus, the risk of contamination is a real one.

4.2 Risks of contamination and mitigation

Risks and potential harm of contamination

Generally, third parties that receive trade secrets in good faith are not **liable for the use of the information in good faith**, i.e., the damages caused by the use of others' trade secrets cannot be claimed. However, depending on national law,[11] as soon as the contaminated company is notified or should have been aware that the information is protected as a trade secret, it should stop using the information. Otherwise, liability could arise for the use after the notice.

The consequences of contamination could be very severe. The potential harms for the contaminated company could include:

- **Loss of investment** if a contaminated company relying on the third party's trade secret has to suddenly cease its use.
- The objective **difficulties in isolating the third party's trade secret** and cleaning the contamination, once the information has spread over the organization.
- The risk of the trade secret holder claiming that the contaminated company is **accountable also for the use of the trade secret prior to the notice** from the trade secret holder, because the company ought, under the circumstances, to have known that the trade secret had been misappropriated. Thus, the trade secret holder might seek injunctions prohibiting sale of the relevant products of the company and/or claim damages.

Mitigation of the contamination risks

The consequence of contamination with third parties' trade secrets could be very serious for the company, and handling the contamination once occurred is extremely burdensome. Therefore, prevention is key to avoid greater damages.

The following **general actions** could be considered to mitigate the risks of contamination.

Invest in the education and training of employees: employees who are well aware of the importance of trade secrets are also able to understand the importance of not letting third parties' information spread within the company. Thus, education and training should focus not only on protection of the company's trade secrets, but also on rejecting unwanted third parties' information.

Keep track of the origin of valuable information: preserving evidence of the date and the circumstances of the acquisition of trade secrets can help to prove that they were present in the organization before the alleged contamination, or that they have been acquired lawfully.

For example, the trade secret holder may demonstrate that certain know-how was developed independently by tracking its research and development activities. In addition, the circumstances of the acquisition of a third party's trade secret may provide indirect evidence for the company to claim that the contamination occurred without its fault.

10 Competitive intelligence is a legal business practice, involving systematic collection and analysis of information from multiple sources. However, if a company acquires trade secret information of competitors through unfair, improper or otherwise considered unlawful means, such investigation constitutes misappropriation of the trade secret.

11 See the overview of trade secret systems in certain countries and regions, available at: https://www.wipo.int/tradesecrets/en/

Monitor the data management and communication system: monitor the data management and communication system to detect any abnormal operations or data flows to outside and within the organization. Note, however, that monitoring information that enters the organization is much harder, since much information flow into the organization is often made by nonelectronic means.

To mitigate the **risk of receiving sensitive information of competitors through competitive intelligence**, a **code of conduct and ethics** that forbid unlawful and unethical practices should be applied vigorously. For example, companies may instruct their employees and business partners **not to use false identities**to gain access to restricted material on websites, at restricted sessions at industry conferences, when ordering a competitor's product, or when using a competitor's service.

Additional mitigation measures that may be taken to minimize the risk of contamination by hiring new employees and through receiving information from collaborators and business partners are explained in Section 5.

4.3 Reacting to contamination

Once the company realizes it has been contaminated with third parties' trade secrets, the company should consider following the general steps outlined below.

- **Understand the situation**: What is the trade secret that was injected in the company? How was it injected? When did it happen? Carry out an internal investigation to locate third parties' trade secrets and secure them to ensure that the company does not use them or stops using them.

Example of an internal investigation

Company A notes that some files with the letterhead of its competitor Company B appear in the data management system of Company A. They include client lists, customer preferences and lists of products purchased in the past. Company A asks its IT team to check who uploaded the documents in the data management system and when. In the meantime, Company A disables access to the documents until the situation is clarified.

- **Involve a legal expert and understand the possible consequences**: the consequences of the contamination will depend to great extents on three factors:
  - the relevance and value of the trade secret;
  - whether the trade secret has been used by the company, the extent of the use and the extent of its spread within the company; and
  - whether the company has innocently received and used the trade secret.

Depending on the above, different scenarios may arise:

- **No use of the received information**: in the less problematic scenarios, the information has never been used and it has not spread within the company. To avoid any inadvertent use of such contaminating information in future, you may isolate and delete such information, or contact the legitimate holder of the information to arrange for its return.
- **Reception in good faith**: if the information has been used, but the company received it in good faith, the company is generally not liable for the past use of the trade secret. The company should check whether it acted diligently to prevent the contamination (for example, whether the company carried out entry interviews and collected entry undertakings from new employees, among others). However, in many countries, once the company acknowledges that the trade secret information was unlawfully acquired, it should generally stop using the information, otherwise it becomes liable for continuing use.
- **Willful or negligent actions**: in the case where the company knew, or negligently ignored, the fact that it acquired the information unlawfully, the company could be found fully liable, also for past acts (see more extensively Part V: Trade secrets in litigation of the Guide).

5. Situations with a high risk of contamination

5.1 Hiring a new employee

Hiring new employees from competitors is one of the two major paths of contamination[12] with a competitor's trade secrets. When a company is contaminated with its competitor's trade secrets, the risk is high that the trade secret holder (competitor) will claim that the contaminated company is accountable, even if it was unaware of the misappropriation. When an employee misappropriates information of his or her former employer, under certain circumstances and depending on the applicable law, the trade secret holder may file action also against the new employer who hired the disloyal employee based on its vicarious liability.[13]

To mitigate the **risk of contamination through hiring employees**, in addition to those described in Section 4.2, several additional measures can be considered.

- When hiring new employees, companies may use an **on-boarding checklist**, requiring them to confirm that they have complied, and will continue to do so, with the confidentiality obligation toward their former employers, such as the return or destruction of any sensitive document and information that belonged to the former employers.
- At the entry interview with new employees , the company should **clearly instruct** that **they shall not contaminate** the company with the trade secret information of their former employers.

These measures are particularly important when hiring high-level employees, who were most likely exposed to highly valuable trade secret information of their former employers.

5.2 Receiving information from collaborators and business partners[14]

In general, knowledge is an essential resource of a company to grow and develop. However, somewhat counterintuitively, receiving trade secret information belonging to others may involve a risk that its future activities will be limited simply because it now "knows" others' trade secrets.

While many scenarios can be conceived, two concrete examples are described below. The first scenario is a situation where a company receives an unsolicited proposal that is seemingly very attractive for advancing its business. The second scenario is a situation where a company engages in a business transaction with another company.

Scenario 1: unsolicited proposals

Let's imagine that a company has significantly invested in an R&D project but has been struggling with a specific problem for some time, causing a delay in the project. An external individual contacts the company with an **unsolicited proposal**, offering a meeting to show, under an NDA, their idea that allegedly solves the problem. Should the company sign the NDA and receive the information?

Maybe they shouldn't be too hasty. A proper **risk assessment**should be conducted, particularly if the company has been **conducting its own parallel projects on the same or similar subject** and is autonomously developing its own trade secrets. Once it receives the trade secret information of others, it may be very difficult for the company to keep that information separate from its own trade secret information.

To avoid this type of inbound risk of contamination, taking into account the risks of receiving the information and its value, one possible mitigation measure is to ask the disclosing party

12 The outline of the measures that may be taken in the situations with a high risk of contamination is found in Sample checklist C, below.
13 Vicarious liability is a form of secondary or indirect liability that is imposed on one party because of its particular relationship with the party who committed a tort. Vicarious liability is frequently asserted against an employer for acts committed by its employees and, according to different national approaches, the employer might be found liable for the employer's wrongdoing.
14 See Part VI: Trade secrets in Collaborative Innovation of this Guide, in particular, Section 2.

to undertake a non-confidentiality agreement, and refuse to receive any information before the**non-confidentiality agreement** is signed.[15]In this way, the company will be fully entitled to use the information received in whatever manner it so wishes. If such a non-confidentiality agreement is concluded, the disclosing party will try to convince the receiving company without disclosing any information that needs to be kept confidential. From this first non-confidential conversation, the company will be in a better position to make a thorough risk assessment of possible contamination by another party's trade secrets and decide whether it is worth taking the risks of signing an NDA and receiving a full set of information, including trade secrets.

Scenario 2: business transactions

Another scenario where there is a very high risk of contamination with others' trade secrets is **business transactions with other parties** (such as external consultants, contractors, potential business partners). These transactions typically involve a transfer of trade secret information from one party to another, and thus can inject in the company the unwanted or unexpected trade secrets.

For example, Company A **outsourced** some research to the research Company B to improve its product. By chance, Company B had already carried out similar research for Company C, a competitor of Company A. On that occasion, research Company B received from Company C useful information, including trade secret information of Company C. Research Company B wants to impress Company A, so it uses such information and suggests in its report to Company A some improvements of the product that in fact takes advantage of Company C's trade secrets.

Has Company A misappropriated Company C's trade secrets? While the answer will depend on the applicable law and the exact circumstances, in general, the decisive point is whether Company A knew or ought to have known that Company B's suggestions were based on third parties' trade secrets. However, even if Company A is considered to be an innocent recipient of the information, Company A might still be required to stop the use of the information. This would mean that Company A could potentially not sell its new product, losing its investments and suffering reputational damage.

Company A could have prevented that unfortunate situation, or at least could have reduced the risks, if it had considered the following measures:

- In the contract with the research Company B, Company A should have **made clear that the company is not interested in receiving anyone else's trade secrets**.
- For the other party to be held accountable for any damages caused by the contamination, **the agreement should include contractual guarantees or indemnification clauses** so that the other party will be liable for any damages caused by the contamination. In the example above, the contract should have provided that in case where the information provided by the research Company B belonged to third parties and was illicitly transferred to Company A, research Company B will compensate Company A for any losses or damages that it might incur.

For research Company B, to reduce the risk of being held responsible for contaminating its client with trade secrets of another client, the company should address conflicts of interests in advance, discuss them with its clients, and set up measures to keep information received from different clients separated.

For Company C, as soon as it is aware that Company A acquired its trade secrets through the service of Company B, it should: (i) notify Company A that its trade secrets have been unlawfully transferred; and (ii) take actions against research Company B that breached its confidentiality obligations, asking for an immediate halt to any further dissemination, return and/or destruction of any documents containing the trade secrets, and compensation for the damages suffered, as detailed in Section 2.5.

15 See also James Pooley (2024). Secrets – Managing Information Assets in the Age of Cyberespionage (2nd Ed.). Menlo Park: Verus Press, pp. 164–165.

Example of the nonchalant consulting firm

Company A would like to improve its business model and be more competitive. It therefore seeks the advice of a consulting firm.

In the past, the consulting firm had advised Company B, a competitor of Company A, on similar matters. At that time, Company B had provided the consulting firm with internal information relating to the market where both Company A and Company B operate. The consulting firm found the information very useful to build a customized strategy leveraging Company B's strengths.

The consulting firm provides Company A with an advisory opinion that uses much of the information provided by Company B to the consulting firm at that time. To increase competitiveness of Company A, the advisory opinion also suggests that Company A implement a new production process.

Management of Company A is very happy with the advisory opinion. They circulate it internally to the various departments of the company and the management approves the new business plan that will guide the company through the next three years. Also, the management approves investment in new machinery and staff training.

After a few months, Company B learns that the consulting firm used its trade secrets to advise Company A. Company B sends a warning letter to Company A, demanding not to use the information that was included in the advisory opinion, including the secret production process.

Company A was innocently unaware that the information belonged to Company B.

Having received legal advice from its lawyers, Company A decides that it has to stop using the production process. This means losing its investment in machinery and staff training. But it cannot take the risk of litigation and an injunctive order by a court.

Regarding Company A's use of other information relating to the market analysis that originated from Company B and was included in the advisory opinion, the situation is more complex. Company A deletes all the documents that include the misappropriated information and informs Company B accordingly. However, the information was used in developing the three-year business plan of the company, which in turn has been extensively used by many departments of Company A. On that matter, Company A and its lawyers conclude that it is no longer possible to "isolate" the trade secrets of Company B and clean the contamination. An open discussion and good faith negotiations with Company B is the only way to avoid litigation. Company A's lawyers approach Company B to discuss a possible amicable settlement of the dispute.

Separately, Company A will also take action against the consulting firm responsible for the contamination.

For Company B, the example shows the importance of due diligence when choosing a party to whom its valuable information will be disclosed, well-drafted confidentiality clauses to protect its trade secrets, and detection of misappropriation as early as possible to minimize damages.

5.3 Sample checklist: Hiring employees and receiving trade secrets of others

The following sample checklist summarizes the measures that can be helpful for reducing the risk of contamination with third party's trade secrets in two specific situations described in Sections 5.1 and 5.2, namely, hiring new employees and receiving confidential information from external parties.

Sample checklist C: Situations with high risk of contamination – Examples of measures

Hiring new employees

1. Assess the risks of being sued by former employers of the new employees.
2. Take general actions to mitigate the risks. For example:
   - train all employees on the importance of not to contaminate the company with others' trade secrets
   - keep track of the origin of valuable information
   - monitor the data management communication system to detect abnormal flows of information.
3. Use an on-boarding checklist, requiring new employees to confirm their compliance with their confidentiality obligations to former employers.

Receiving information from collaborators and business partners

1. Carry out a risk assessment of receiving confidential information from others, particularly where the company is working on the same or similar subject matter.
2. Make clear to collaborators and business partners that the company is not interested in receiving anyone else's trade secrets.
3. Include contractual guarantees or indemnification clauses in contracts so that another party will be held liable if it contaminates the company with a third party's trade secret.

6. Strategic exploitation of trade secrets

6.1 Exploiting the economic value of trade secrets: modalities

Similar to other intellectual property assets, based on strategic analysis of the value of a trade secret and the competitive advantage that it may bring to the company's business, the trade secret holder may determine the best way (or ways) of exploiting their trade secrets. There are different ways that trade secret owners can exploit the economic value of trade secrets.

Exclusive exploitation by the trade secret holder

Trade secret holders may **use the protected information exclusively by themselves**. They may choose to exclusively research, develop, manufacture and sell products and services having features covered by their trade secrets. They choose to do so because the success of their business comes precisely from the fact that a trade secret holder is the only one who possesses that information and thus can use it.

Non-technical trade secret information, such as sensitive business information relating to customers and vendors, pricing, business strategies etc., is often used exclusively by trade secret holders. However, there can be a situation where sharing confidential business or commercial trade secret information with another business partner makes more sense: that is, when sharing such information brings more competitive advantage to the trade secret holder than keeping such information by itself, as illustrated below.

Allowing certain use of trade secrets by others under the control of the trade secret holder

Trade secret holders may allow certain parties to use their trade secrets for certain purposes, during a certain period, within a certain geographical area, and under any other conditions (for example, payment of a licensing fee).[16]

16 In practice, trade secrets are licensed in conjunction with other IP rights or in the context of a broad technology agreement. It is rare to license a trade secret on its own.

As already illustrated in some examples described in this Part, there are various situations where trade secret holders choose to share their sensitive information with their business partners, suppliers and customers. Under certain circumstances, sharing of trade secret information may lead to improvement of business efficiency, higher quality of products and services and greater commercial success.

For instance, to **generate revenue** and/or **gain business efficiency**, trade secret information may be shared with:

- **business partners** for collaborative R&D, marketing, and other projects
- **local manufacturers** of the company's products in foreign countries
- **franchisees** pursuant to franchise agreements, and
- external contractors who carry out certain **outsourced** business processes of the company.

The licensing conditions are agreed between the parties on a case-by-case basis. The degree of authorized scope of use of the trade secrets as well as the terms of payment (e.g., percentage of profits, fixed license fee or lump-sum payment) are essential elements in licensing agreements. To require the licensee to maintain secrecy of the trade secret information, the licensor may:

- seek the right to audit the licensee's compliance with the terms of the licensing agreement, and/or
- require confidentiality of the licensed trade secret information even after termination of the agreement.

In particular, with respect to franchise agreements, the franchisor may consider the possibility of granting franchisees to access a tangible product that pertains to trade secret information (sauces with special ingredients) rather than disclosing the trade secret information as such (detailed information about the ingredients).

In addition, a company may be inclined to share its trade secret information with **external consultants or advisory service providers** who need the company's sensitive information to **deliver high quality services** to the company.

Due to the fact that secrecy is a prerequisite for trade secret protection, the common challenge for exploiting trade secrets through licensing is to sufficiently define the licensed trade secrets and to manage the risk of breach of non-disclosure or of confidentiality before and during the negotiation of the license and after the conclusion of the license (see Section 2.3 on contractual measures, 3.2 on risk of misappropriation by sharing information with an external party and Section 4 on avoiding contamination with others' trade secrets).

Assignment of trade secrets

Trade secrets can **be assigned**, or put differently, the legitimate control over the trade secret information can be transferred to another party.

Oftentimes, the very reason for carrying out certain corporate operations, such as mergers and acquisitions, is the willingness of the investor to acquire know-how and trade secrets held by the target company. Starts-ups are often acquired because of their significant assets in IP rights, including trade secrets.

Fundraising

Depending on the applicable national law, trade secret holders may negotiate, create and perfect **security interests in trade secrets**. They may serve as an additional means to raise capital from private or public institutions. Unlike other IP assets, maintaining the secrecy of trade secrets is required for their securitization.

Tax and accounting

Under certain conditions and in some jurisdictions, trade secrets may be:

- included in the **company's accounting**, thus contributing to the overall corporate value
- considered for transfer pricing purposes, if used throughout the same group[17]
- covered by a tax relief measure, such as "innovation box" or "intellectual property box," which is a special corporate tax regime to incentivize corporate research and development activities.

6.2 Continual alignment of the exploitation strategy with business needs

Dynamic notion of trade secret exploitation

Trade secrets are an integral part of IP assets. Typically, in the technology sector, a small or medium-sized company may own several patents, copyrighted materials that may or may not be public, industrial designs of their products and trademarks that distinguish their products. In addition, it may hold trade secret information surrounding their products and their commercial activities. Therefore, strategic use and exploitation of trade secrets cannot be considered in isolation. Rather, they should be considered in conjunction with other IP rights.

The protected subject matter of registered IP rights is usually "cast in stone" at the time of registration, or in the case of copyright, at the time of creation. However, **trade secrets can evolve together with business activities**, which constantly generate new valuable information.

At the same time, trade secrets are more vulnerable than other types of IP. Even if it does not have a statutory limited term of protection, a lifespan of a particular trade secret may be short, depending on its nature (such as the next month's product introduction) or handling of information that can potentially lead to premature disclosure. Once the trade secret information is leaked, its value for the trade secret holder can be significantly reduced or its legal protection is entirely lost if it is widely disclosed. Trade secrets can also be lost when the information no longer has value derived from secrecy.

This means that the information in the company's **trade secret pool is constantly changing within the IP portfolio**.

In addition, the strategic use and exploitation of trade secrets should be **considered in conjunction with the changing market and company's business needs**, since they also have an influence on the value of a particular trade secret information in the company's pool.

Consequently, the "strategic" management and exploitation of trade secrets is a **dynamic concept**, both in terms of its **value** and **its risk of loss of protection**.

Therefore, there is aneed to **regularly review trade secret assets** in the context of the overall IP portfolio, and to **align** the trade secret management and exploitation strategy with the evolving business needs in an ever-changing market. The review may be conducted broadly in three steps:

- **Assess** any changes in the pool of trade secrets and how the changes affect the company's competitive advantage (i.e., value of the trade secrets) and risk, in the context of other IP assets.
- **Review** whether the current trade secret protection plan and measures as well as trade secret exploitation strategy are still appropriate.
- **Update** the protection plan, measures and exploitation strategy, if necessary.

17 Transfer pricing accounting occurs when one division provides goods or services to another division of the same company and charges the latter division. Using the differences in the tax rates among countries in which the parent company and subsidiaries locate, transfer pricing is utilized to reduce the tax of the parent company.

Exploitation strategy beyond the trade secret system

In reviewing and updating the trade secret exploitation strategy, one possibility is to seek different or additional revenue stream(s) from the **exploitation modalities available in the trade secret system**. Some questions that may be addressed are:

- **Will the trade secret information continue to provide competitive advantages because of its secrecy?**
  Technological trade secret information can become obsolete at some point in time due to the technological development inside the company or elsewhere.
  New technologies may reduce competitive advantages by offering competitors the means to independently create the same information with much less effort and subsequently duplicate the company's products or services in a shorter time and with less risk.
- **Will the trade secret information continue to remain secret?**
  Reverse engineering and independent creation of the same information are usually not regarded as trade secret misappropriation in many countries. If a technological gap between the trade secret holder and its competitors diminishes, the likelihood of the competitors lawfully obtaining the information through reverse engineering or independent creation of an invention increases. It may lead to the trade secret no longer having value, and even worse, the competitors might obtain patents on the invention and may seek to preclude the company from using the trade secret.[18]

Another possibility for trade secret holders is that, instead of maintaining trade secret protection, they may seek **revenue stream(s) from the exploitation of other IP rights**, such as patents or copyright.

Trade secret to patents

Since trade secret information is protected under confidentiality, it is generally not part of prior art under patent law in many countries.[19] Therefore, in those countries, trade secret holders may be able to **switch from trade secret protection to patent protection**, if it meets their business needs. Part III: Basics of trade secret protection of this Guide provides more information on the differences between patent and trade secret protection. The factors that may be considered in making a choice described in Part III are also applicable in this situation. In essence, both**legal factors** (eligibility of protection, the scope of rights and their duration and geographical coverage) and **business factors** (costs, resources, market conditions and reputational effect) are relevant.

Trade secret and/or copyright

Copyright protection arises automatically in an original work once it is created and fixed in a medium. As long as the expression of such work is kept confidential and meets the requirements for trade secret protection, it can be protected by both copyright and trade secret law. However, depending on business needs, the trade secret holder may be able to **switch from such dual protection to the combination of patents and copyright protection** in case of software. It may also considers**shifting to copyright protection only**, if, for example, open source software is in line with strategic business direction.

Renouncing trade secret protection

Finally, it is also possible that the rational business consideration leads to the conclusion that the company will relax trade secret protection measures and also not seek any alternative protection. Maintaining trade secrets is not an end in itself. They should support a competitive advantage of the business, whether it is for technological competitiveness, monetary rewards,

18 In many countries, the prior-user exception to patent rights may allow the trade secret holder to continue using the information, although the scope of the exception may be limited.
19 In the United States of America, in general, a patent applicant's sale of an invention, more than one year before the effective filing date, to a third party who is obligated to keep the invention confidential destroys the novelty under the patent law (on-sale bar), and thus the applicant cannot first enjoy trade secret protection relating to inventions on sale for many years, and then switch to patent protection for the same invention.

or reputational advantage. If you renounce trade secret protection without seeking patents, you may consider actively publishing that information so that your competitors will not be able to obtain a patent on that subject.

7. Valuation of trade secrets

7.1 Trade secret valuation – what is it for?

To make various business decisions around management and exploitation of IP in diverse circumstances of business transactions, having an idea of the value of your IP assets, including trade secrets, will be helpful. Valuation of trade secrets provides trade secret holders with **additional information that may assist them to take informed decisions** relating to trade secret management, enforcement, and licensing, or even switching from trade secrets to patent protection. For example:

Cost-benefit analysis for internal IP management

IP valuation may allow trade secret holders to analyze costs and benefits of trade secret protection of certain information, and to maintain their IP portfolio in line with their strategic business goals. This is particularly so if there exists an alternative means of protection (e.g., patents).

Licensing and franchising

Before entering negotiations on licensing of IP assets, including trade secrets, having a thorough understanding of their relative value will help trade secret holders make more informed decisions on the terms and conditions of the licensing agreement, including royalty rates. In franchising, both franchisor and franchisee need a thorough understanding of the value of the relevant IP assets.

Settling disputes

Knowing the value of information assets can have a positive effect on making strategic decisions when those assets are threatened or misappropriated. For example, the trade secret holder may need to decide whether to pursue litigation, to opt for alternative dispute resolution, or to offer a license to the alleged infringing party. Valuation also plays an important role in calculating damages suffered due to the unauthorized acquisition, use or disclosure of the trade secret.

Attracting partners

For business collaboration and transactions, such as a joint venture, strategic alliance, merger or acquisition, valuation can facilitate better understanding about how the assets of all parties contribute to the partnership.

Secure financing

Venture capitalists and other potential investors look for maximum return and minimum risk. Therefore, they need to know the value of the company's IP before investing in it. To use trade secrets as collateral to obtain financing, their valuation separately from the company's other assets may be necessary.

Terminologies: price, value and valuation

In the context of IP management, it is important to distinguish the price and value of an IP asset, although they can be used interchangeably in our daily conversation. "Price" is typically defined as what a buyer is willing to pay, in an arms-length transaction, based on the perceived value of the product.

On the other hand, "value" is an abstract, but deterministic quantity whose calculation is based on a systematic and established set of methods.

Thus, the "valuation" of IP does not determine the price tag for an IP asset, which can be affected by many other aspects of the transaction.

7.2 Valuation methods

The valuation methods that can be used for trade secrets are the same as those applied to IP assets in general. The principal methods for valuation of IP assets are: (i) cost method; (ii) market method; and (iii) income method.

Cost method

The cost method seeks to establish the value of the asset by calculating the cost of creating or replacing a similar asset.

This method values trade secret information by aggregating the expenditures incurred or that would be incurred in developing or creating the asset or a similar product or service, such as costs relating to labor, materials, equipment, R&D, testing etc. It seeks to determine the value of a trade secret at the time of misappropriation by aggregating the direct expenditures and opportunity costs involved in its development. It also considers technological and economic obsolescence that may affect its value.

Strengths of the cost method

The cost method can be used in situations where the misappropriator is currently not generating any income, such as technology at an early stage of development.

It can also be useful when development costs can be easily calculated and the cost of reproduced is low (e.g., software).

If the income stream or the economic benefits of the IP asset cannot be reasonably or accurately quantified, the cost method may also be helpful.

Weaknesses of the cost method

The cost method focuses on past expenses rather than on future profits, and therefore it does not necessarily reflect the market potential of the asset. This is particularly true for trade secrets created through experimental research and development, where huge investments can produce many failures, while they can also lead to revolutionary inventions with huge commercial success. Accordingly, the cost method does not fit well in certain sectors, such as pharmaceuticals.

A value assessment based on costs could produce misleading results and underestimate or overestimate the value of the trade secrets.

Market method

The market method seeks to determine the value of an asset by comparing it with a comparable asset available in the market. The value is determined by comparing both the assets in similar transactions under comparable circumstances.

The key to such assessment is to find a good comparable in the market, i.e., similar transactions that concern similar products or service, which could be considered as a reference. Once a comparable is identified, adjustments that take into account the differences in the two situations are generally needed.

Strengths of the market method

- Simple method using market-based information
- Can be useful if a good comparable (such as licensing agreements related to the same subject matter) is available.

Weaknesses of the market method

- Difficult to find a good comparable for trade secret value, because:
  - every secret is usually unique
  - in general, the value of secrets derives from their newness or originality, but they must be not generally known or readily accessible.

Income method

The income method is one of the most commonly used methods for IP valuation. To determine the present value of trade secrets, it focuses on the economic income that the asset is expected to generate in the future.

In determining economic incomes, the following parameters are used:

- projecting the revenue flow (or cost savings) generated by the trade secret over its remaining useful life
- adjusting the revenues/savings against the investments made for the development of the secret (e.g., costs of labor, materials, capital investment etc.)
- discounting the expected revenues to present day value using a "discount rate."

Strengths of the income method

- This method is easiest to use for assets with established cash flows, for those whose future cash flows can be estimated with some degree of reliability, and where a proxy for risk that can be used to obtain discount rates is available.
- It captures well the value of trade secrets that generate relatively stable or predictable cash flows.

Weaknesses of the income method

- The discounted cash flow (DCF) method does not consider the total risk of the investment. Instead, it only considers the systematic component of that risk in the form of market determined discount rate.
- The DCF assumes that the investment in the secret is irreversible, irrespective of future circumstances.
- It does not capture the various independent risks associated with trade secrets (e.g., a legal risk of losing protection due to leakage and public disclosure or a risk of independent development of the same information by a competitor). All risks are assumed to be appropriately accounted for in the discount rate and the probability of success.

In summary, regardless of the valuation method used, the valuation process requires gathering varying information about the trade secret as well as an in-depth understanding of the market, industry and specific business, all of which directly affect the utility of the results of the valuation.

In general, **valuation of trade secrets is inherently more difficult** than other intellectual property due to their confidential nature. More specifically, it is challenging to separate and identify a revenue flow or costs that can be exclusively credited to trade secrets. Each of the three major IP valuation methods has its general strengths and weaknesses. Which valuation method, or a combination of the methods, to be applied should be determined **case by case**.

Part V: Trade secrets in litigation

Topics covered in this Part:

- **What to do if you discover trade secret misappropriation or contamination**
- **Legal remedies and preliminary injunction**
- **Alternative dispute resolution**
- **Building a strong case, burden of proof and evidence**
- **Defense against misappropriation claim**
- **Preservation of trade secrets in court proceedings**
- **Cross-border issues**

1. Overview

Ideally, leakages and contamination of trade secrets should be avoided from the outset through a good trade secret management policy. However, even with the highest security standards, breaches happen, and trade secret holders need a plan for how to react. Part V of the Guide provides an overview of the options available when trade secret misappropriation occurs. Pursuing litigation to remedy trade secret misappropriation is just one option available for trade secret holders. Thus, this Part also addresses other options that may support resolution of disputes.

Trade secret misappropriation can happen due to espionage or cyberattack, but most frequently, it happens in day-to-day human behaviors in a business. Misappropriation occurs most often through current or former employees, but also in business relationships such as a potential acquisition or license, or through supply chains. When misappropriation occurs, it is very difficult for trade secret holders to know all the relevant facts, since misappropriation itself happens in secrecy, often without any indication that there has been a loss. In a way, by definition, finding a right track to counter the misappropriation is a difficult task.

As the TRIPS Agreement only provides a minimum standard that WTO members need to implement in their legislations (see Part III, Section 1.3), the enforcement of trade secrets through litigation, remedies and procedural rules varies significantly from one jurisdiction to another. Therefore, this Part provides a general overview of trade secret litigation, identifying the most important commonalities, differences, major trends and recurring issues in the various regional and national approaches. While it mostly focuses on civil enforcement, criminal and administrative enforcement issues are also addressed towards in this Part.

The variation in national trade secret laws as well as procedural rules makes navigating trade secret litigation challenging. Therefore, a more detailed overview of enforcement practices of some countries can be found on the WIPO website,[1] which covers both civil and criminal enforcement. Furthermore, the Annex to this Guide contains a list of reference materials that

1 See the overview of trade secret systems in certain countries and regions, available at https://www.wipo.int/tradesecrets/.

are published by national/regional authorities and online materials that provide country-by-country analysis of national trade secret enforcement systems.

2. What you can do when you realize that a trade secret has been misappropriated: to sue or not to sue

2.1 What is misappropriation?

When patented inventions or trademarks are used without authorization of their owners, it is called "patent infringement" or "trademark infringement." When trade secret information is used without authorization of the trade secret holders, this is called "misappropriation" and those who carry out the misappropriation are called "misappropriators" in this Guide.

As mentioned in Part III: Basics of trade secret protection, trade secret protection does not confer exclusive rights, but regulates parties' behavior to prevent wrongful conduct. The basic idea of prohibiting others from securing unfair commercial advantage by acquiring, using or disclosing trade secrets of another person in a wrongful manner is expressed in national laws in different ways. However, in essence, when the **acquisition, disclosure or use** of the information covered by the trade secret protection occurs by **unlawful, improper, dishonest or unfair** means, it is generally deemed to be misappropriation.

When misappropriation occurs, the misappropriator may sell or license (or otherwise disclose) the trade secret to another party, and that party may further use and disclose the trade secret information, and so on. Therefore, misappropriation of trade secrets may happen in scenarios that involve other parties beyond the trade secret holder and the direct misappropriator.

In essence, there are two scenarios where these other parties may get involved in misappropriation:

1. Third parties **who knew, or were grossly negligent in failing to know**, that the trade secrets had been misappropriated. In general, acquisition of trade secret information by third parties who knew, or were grossly negligent in failing to know, that the trade secrets had been misappropriated is considered misappropriation. In many countries, further use or disclosure of the information by these third parties also constitutes an act of misappropriation.
2. Third parties without knowledge of misappropriation (**innocent or good-faith recipients**). In general, if third parties were genuinely not aware that the information they received was misappropriated information, the **acquisition** of that information is not considered misappropriation. However, whether their subsequent **use or disclosure** is considered.

In many countries, in cases where unauthorized persons make, sell etc. **products resulted or benefitted from unlawful acquisition, use or disclosure** of trade secrets, in general, these products can be subject to injunction claims and other requests for relief.

2.2 Investigate and understand the situation

An effective trade secret management policy should provide guidance on how to handle the situation when the trade secret holder realizes that misappropriation has occurred. Litigation is not always the best solution to react to misappropriation. However, in order to preserve its option to seek remedies through litigation, the trade secret management should:

- preserve evidence so that the trade secret holder will be able to substantiate its claims in litigation
- investigate facts without alerting the alleged misappropriators who might be inclined to destroy evidence of their behavior, and
- take emergency measures to mitigate immediate harm.

Details of these steps are found in Part IV: Trade secret management, in particular, Section 2.4.

2.3 Out-of-court solutions or litigation: elements to consider

After having preserved the evidence, understood what happened and secured the situation to prevent further violations, the trade secret holder generally has three options for how to react:

- pursuing an amicable settlement of the dispute
- starting litigation, or
- not taking any action.

Factors in assessing whether or not to go to court

The choice depends on a thorough assessment of a multitude of factual, legal and business considerations. These could include the following:

Legal restrictions: the options to react could be contractually or legally limited.

Example of restricted options of recourse

If the misappropriation was carried out by an employee or an external contractor, contractual obligations could foreclose or limit the possibility to obtain certain remedies before specific courts, could impose applicable law or could force resort to alternative dispute resolution mechanisms (see 3.4).

The value of the trade secret and the seriousness of the violation: generally, the higher the value of the trade secret and the more serious the misappropriation, the stronger the counter-reaction of the trade secret holder will be.

Example of different responses to different trade secret value

If a single employee transfers a few confidential files onto their personal device, a formal warning, a reminder of the internal policies and making sure that the employee deleted all the confidential files could be sufficient. In contrast, where several employees quit and move to a competitor after having massively downloaded the former employer's confidential files on their last days of work, filing court proceedings by way of urgency to obtain seizures and injunctions against the competitor and the former employees could be preferable.

Need for provisional measures and risks of counter-reactions: it can happen that the trade secret holder can demonstrate some suspicious facts but has no solid evidence to build a strong court case. In that situation, many legal systems provide specific judicial inspection orders (see 4.2.3). Depending on the legal system, *ex parte* judicial inspection orders and preservation of evidence are possible. In these cases, the other party will not be heard before the court orders a provisional measure. This is particularly useful where any delay or alerting the other party may result in irreparable harm or evidence destruction.

Should the trade secret holder want to rely on provisional measures, in particular *ex parte* provisional measures, trying to pursue an amicable solution first (for example, by sending a warning letter) would put the defendants on notice and could undermine the effects of any evidentiary measures sought at a later stage.

Possibility of counterclaims or "unclean hands" objections: before taking action, it is advisable to double check whether secrecy measures have been applied properly according to the applicable law so that the trade secret information has been appropriately maintained. Missing this step could be critical. For example, if such measures have not been taken, the defendant could argue that the information no longer meets the requirements for trade secret protection, because the plaintiff has not taken reasonable steps to keep it secret.

As a separate matter, if the defendant could prove that the evidence of misappropriation submitted by the trade secret holder was collected unlawfully, courts may consider it inadmissible or unreliable (see 4.3 with respect to collection of evidence).

Costs of litigation: the costs of litigation (in terms of money, time and effort) must be weighed against the value of the trade secret and the benefit of litigation, including a potential benefit of providing a message to employees and others that the company is serious about protecting its information asset. The costs will depend on the place of litigation, the remedies sought and the kind of proceedings. A cost–benefit analysis of the litigation should be assessed case by case. It is generally advisable to do this analysis also in view of the company's mid- and long-term business strategy.

Tip: Consider long-term risks and costs

Sometimes, a "soft" reaction that can save costs on litigation in the short term can become more expensive for businesses in the long term, since it can encourage repeated misappropriation of trade secrets.

Likelihood of success: before starting court proceedings, the likelihood of success needs to be evaluated. A main issue to consider is what kind of evidence the trade secret holder can provide (see Section 4).

Public relations: sometimes, a trade secret holder wants to avoid any publicity relating to trade secret misappropriation cases. In addition, depending on the relevant national rules, the risks of trade secret information becoming public during the court proceedings or in the publication of judgments might influence the decision of a party to start court proceedings (see Section 6).

Out-of-court options

If the trade secret holder decides not to pursue court proceedings, other possible reactions may be:

Sending a warning letter: if the trade secret holder does not fear the destruction of evidence following notice, a warning letter can be a good option to:

- remind misappropriators of any confidentiality and non-disclosure obligations;
- demand that the misappropriator cease the improper behavior;
- demand the return or destruction (with provision of evidence) of the misappropriated materials; and
- make the misappropriators undertake non-disclosure and non-use of the misappropriated information.

License offer to the misappropriator: a trade secret holder may offer the misappropriator a license for its use of the misappropriated trade secrets. However, this must be done with caution and preferably with extra fees to compensate for the initial trade secret misappropriation. Otherwise, the market could learn that the best way to get a license on the trade secret is misappropriating it in the first place, and then obtaining a favorable license.

Proposing an alternative dispute resolution mechanism (see Section 3.4): a mix of court and out-of-court solutions may often be effective. Sometimes, reaching an amicable solution may become more likely after court proceedings have been initiated. If a court proceeding would likely turn out in favor of the trade secret holder, the misappropriator will face more pressure to settle. The trade secret holder may also get better terms for the settlement in that way, which could potentially compensate for the cost of litigation.

No action: the trade secret holder could also take no action. This could be appropriate if, for example, there is not enough evidence of the misappropriation, or costs of litigation are too high. However, such a decision must be made with the clear understanding that inaction could mean letting the competitor gain a competitive advantage and benefit from its unfair conduct. It could also mean that the information could lose its legal status as a trade secret.

2.4 Considerations in advance of litigation

The legal basis of trade secret protection in the relevant jurisdiction

Trade secret holders have the possibility to seek legal remedies for trade secret misappropriation, depending on the legal basis of protection under applicable national laws. For instance, trade secret protection may be based on specific trade secret laws or unfair competition laws or common law duties of confidence, or determined by contracts in accordance with applicable contract law. In some countries, trade secrets are considered as intellectual property subject to specific remedies. Naturally, to rely on a breach of contractual confidentiality clauses, enforcing a trade secret in court may not be possible without having such a clause in place. In the absence of such a clause, trade secret holders need to base their claims on other legal basis of trade secret protection.

Where possible, a trade secret holder may also combine multiple causes of action. However, a different legal basis generally means different requirements to access legal protection. For example, a contractual basis for protection implies that the parties concluded a valid and enforceable contract according to the applicable national contract law, while under unfair competition law, the misappropriator generally needs to be a competitor of the trade secret holder.

Both the enforceable legal claims and the existence of their requirements need to be assessed on a case-by-case and country-by-country basis.

Entitlement to sue

Generally, the legitimate holder of a trade secret is entitled to start proceedings for trade secret misappropriation (entitlement to sue). However, other persons in lawful possession of the information may also be entitled. Who and under which circumstances a natural or legal person is entitled to sue will depend on the respective jurisdiction. Often, licensees[2] may also have entitlement to sue, although it depends on the licensing contract and the applicable national law.

Examples of differences in entitlement to sue

Some countries, such as China, deem at least exclusive licensees are entitled to sue, while in some other countries, such as Argentina, licensees are considered not to have such entitlement, unless expressly authorized by the licensor in the license agreement. In case of work for hire, it is typically the employer who is exclusively entitled to sue as the legitimate holder of the information produced or obtained by employees in the course of employment (for example, Fraser v Evans [1969] 1 QB 349 (UK)).

Statute of limitations

As for other legal claims, proceedings seeking remedies for trade secret misappropriation can only be brought by trade secret holders within a certain amount of time from their knowledge of, or the occurrence of, the act of misappropriation. Since no legal certainty and "legal peace" could be reached without the statute of limitations, generally, trade secret claims may be time-barred. However, rules relating to limitation periods in trade secret matters are not uniform internationally.

- **Duration of the limitation period**: in general, the duration of the limitation period for large scale misappropriation or for misappropriation that is considered a criminal offense, will be longer than for civil remedies. Often, the statute of limitations in different countries ranges between three to six years.

2 While the academic discussion on whether a trade secret is property or not may affect the legal qualification of the subject matter of the contract, it is almost undisputed that trade secrets (and confidential information not amounting to trade secrets according to the law) are capable of being assigned, transferred or licensed.

- **Start, interruption or suspension of the limitation period**: generally, the limitation period begins with the date of the alleged misappropriation, or the moment when a trade secret holder obtained the knowledge of the alleged misappropriation or could have obtained such knowledge with due care.
- There are also circumstances such as the initiation of legal proceedings, sending certain communication to the other party, or the acknowledgement of the misappropriation by the other party, which may suspend[3] or interrupt[4] the limitation period.

3. What relief is available in court or in alternative fora

Trade secret holders have the possibility of seeking different types of relief measures and remedies for misappropriation. This Section discusses some of them in more detail.

3.1 Injunction

By an injunction, further acts of acquisition, disclosure or use of trade secrets can be prohibited. In cases of products that have been tainted by misappropriation, an injunction may also prohibit production, offering for sale, placing on the market or use of those products, or importation, export or storage of those products for such purposes.

Courts generally impose recurring penalty payments in the event of non-compliance with injunctive orders. In addition, many countries consider non-compliance with the court's order as a crime.

Whether and to what extent courts have discretion to grant injunctions is a highly debated issue that goes beyond trade secret law. In common law countries, injunctions are traditionally intended as discretionary remedies, equitable in nature, that are not granted automatically but only if the court deems them appropriate, considering the specific circumstances of the case. In civil law countries, on the contrary, injunctions are traditionally intended as automatic or quasi-automatic remedies once infringement is found. The diverging positions seem to have come closer in recent years, and in trade secret matters, there may generally be a wider consideration of proportionality than in patent law, for example.

Case example: Heraeus v. Zimmer Biomet (Italy)

This case involved the misappropriation of trade secrets for a medical technology product. The Court of Milan found that granting an injunction would negatively affect third parties, including public health institutions, that had agreements with the misappropriator for the supply of the medical product concerned.

Considering proportionality, the Court granted an injunction order with a grace period of one year (i.e., the injunction would only enter into force after one year). The Court deemed one year was sufficient to safeguard the continuity of ongoing supplies to public administrations and hospital facilities by carrying out urgent public tenders for the purchase of equivalent products and training their medical staff. During the grace period, monetary damages were still applicable as an alternative to an immediate injunction.

The same case was litigated in several countries. While the proportionality considerations are case specific, reportedly, the Italian case is unique in granting a grace period.

Source: See Heraeus Medical GMB - Heraeus S.P.A. v. Zimmer Biomet Italia S.R.L.- Unknown company, Tribunale di Milano, Sezione specializzata in materia di impresa, May 16, 2019, in Trade Secrets Litigation Trends in the EU (2023). European Union Intellectual Property Office, pp. 89 ff. Available at: https://data.europa.eu/doi/10.2814/565721.

3 Suspension freezes the time already elapsed without erasing it and hence, when the event causing the suspension ceases, the limitation period begins to run again from when it had stopped.
4 Interruption of the limitation period erases the period acquired up to the interruption and starts a new period of the same duration.

Preliminary injunction

Preliminary injunctions are granted by way of urgency, and therefore are issued in shorter time and at lower costs than injunctions following a trial on the merit. To prevent loss of secrecy of the information, preliminary injunctions are particularly important in trade secret matters.

In many countries courts may grant preliminary injunctions before or during the proceedings on the merits if:

- there is likelihood of success in the proceedings on the merits;
- there would be severe or irreparable harm suffered in the time necessary to obtain an injunction following final determination of the merits; and
- the applicant has demonstrated that the matter is urgent.

Generally, preliminary injunctions are temporary and aim to preserve the trade secret holder's right only for the time needed to get a judgment on the merits, in which the court may grant an injunction after the full assessment of the case. Therefore, trade secret holders are required to start proceedings on the merits within a certain time after the urgency proceedings.

In cases of special urgency or when there is a risk that the enforcement of the injunction will be frustrated if a prior notice is given, many countries provide for *ex parte* **preliminary injunctions** without the alleged misappropriator being heard.

In many countries, courts have discretion to grant a preliminary injunction and may consider factors, such as irreparable harm to the trade secret holder, balance of convenience and balance of hardship (in essence, balancing the relative positive or negative effect on the parties if a preliminary injunction is granted or refused). In order to balance the rights of the alleged misappropriator, courts in many countries, such as Belgium, Japan, Poland, Sweden and the United Kingdom, may require an appropriate guarantee or bond from the trade secret holder to ensure that the defendant may be compensated for possible losses by the grant of the preliminary injunction, if the proceedings on the merits show that the preliminary injunction should not have been granted.

In addition, in accordance with Article 50.4 of the TRIPS Agreement, in the case of *ex parte* preliminary injunction, the affected parties shall be given notice, without delay after the execution of the measures, and a review shall take place upon request of the defendant.

As an alternative to a preliminary injunction, in some EU member states, for example, it is also possible that courts require from the alleged misappropriator an appropriate guarantee of payment for the continuation of the alleged unlawful use of the trade secret to ensure that a trade secret holder may obtain compensation, should the trade secret holder's right be found violated in the subsequent proceedings on the merits.

Time limit of the injunction

Generally, injunctions last **as long as the information remains a trade secret**. Once the information loses its secret nature through, for example, disclosure, and consequently loses its trade secret status, the injunction may be lifted.

Obviously, once the misappropriator has gained knowledge of the trade secret, it cannot be erased from his/her mind. If trade secret protection has expired and the injunction has lapsed or been lifted, the misappropriator can use the misappropriated knowledge in the market with a lead time advantage over others who have just learned of the information. Therefore, in some countries such as Australia, Canada, Singapore and the United Kingdom, a so-called "**springboard injunction**" may be granted, considering that an injunction against a competitor should at least last the time it would otherwise have taken to lawfully obtain the information. Hence, in some cases, a court may extend the injunction even beyond the life of the trade secret, until the rest of the market has caught up. Generally, the duration of the springboard injunction is calculated as the time that the infringer would have taken to legitimately reverse-engineer and obtain the trade secret or independently discover the trade secret.

Injunction to limit subsequent employment

In those jurisdictions that allow non-compete agreements between employers and their employees, in order to indirectly protect their trade secrets, employers may restrict employees from competing with them after they leave the company. However, even without such agreements, when the trade secret misappropriation is carried out by a former employee who joins a competitor, the trade secret holder could try to prevent the employee from working for the competitor to avoid the threat of further disclosure and use of the trade secret. As the employer's rights to trade secrets and the employee's right to professional mobility must be well balanced, in general, such **injunctions that limit the employee's subsequent employment opportunities** are granted only in extreme circumstances.

Example of injunction limiting subsequent employment

The Supreme Court of the Republic of Korea granted an injunction limiting the subsequent employment of a former employee even in the absence of a non-compete agreement, because the Court deemed it impossible to protect the former employer's trade secret without imposing this prohibition.

Source: See Supreme Court of the Republic of Korea, Judgment of July 16, 2003, Case No. 2002ma4380.

Under the so-called inevitable disclosure doctrine, which is applicable in, for example, Argentina and some states in the United States of America, a plaintiff may obtain an injunction if it proves that a former employee will inevitably use or disclose the former employer's trade secret during the new employment, causing injury to the former employer as a result.

Example of inevitable disclosure

The inevitable disclosure doctrine was applied where a high-level executive resigned to work for a competitor in the same niche market, lying to the employer about his future plans. The court concluded that it would be impossible for the former employee to perform their new employment without relying on the knowledge of the former employer's trade secrets, or without disclosing them to the new employer.

Source: See PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1269 (7th Cir. 1995), citing Teradyne, Inc. v. Clear Communications Corp., 707 F. Supp. 353, 356 (N.D.Ill. 1989).

3.2 Monetary remedies

Monetary remedies are the second major tool for trade secret holders against trade secret misappropriation.

As seen previously, the legal basis for protecting trade secrets could significantly vary in different jurisdictions and many countries do not have specific trade secret provisions. Instead, they rely on different causes of action such as claims for breach of unfair competition law, breach of tort law, breach of contract, breach of confidence and breach of equitable obligations under common law. Such differences also affect related claims for damages. For example, in case of breach of contract claims, the quantification of damages is mainly based on the agreement. Additionally, contractual liability is often limited to damages that were foreseeable when the parties entered the contract, while such limitation is generally not provided for tort law damages.

However, despite the different legal basis, there is a broad consensus on the monetary measures available, at least in their core features. First, there must be a **causal link** between the alleged trade secret misappropriation and the losses claimed by the trade secret holders or

unjust enrichment of the misappropriator. Second, **trade secret holders bear the burden** of proving the amount of the damages. In practice, quantification and proof of damages can be a complex task.

Monetary remedies can be classified according to their functions.

Compensatory damages

The purpose of compensatory damages is to place the injured party in the same position as if the injury had never occurred. Therefore, in the case of trade secret misappropriation, the trade secret holder may claim compensation for the damages it has suffered by losing control over the information. Generally, compensatory damages include loss suffered and lost profits caused by the misappropriation.

Loss suffered (potentially including non-economic damages)

The "loss suffered" may include, depending on national approaches, the lost investment for, for example, R&D of products or delivery of services to which the trade secrets pertain, and the expense incurred for investigating misappropriation and preparing for litigation.

Lost profits

Quantifying lost profits requires operating a counterfactual analysis consisting of calculating the difference between the cash flows in the factual scenario (i.e., the actual cash flows after the misappropriation occurred) and in the counterfactual scenario (i.e., the foreseeable cash flows had the misappropriation not occurred).

Reasonable royalties

Another way to calculate damages is relying on the so-called "reasonable royalty" that a willing licensor and a willing licensee would have agreed on for a license in a hypothetical negotiation. Therefore, the reasonable royalty should reflect the market royalty, which is the royalty usually practiced in the marketplace. A reasonable royalty may be based on a running payment, a lump sum or a combination of both. Its application to trade secret cases, however, may face particular challenges due to the confidential nature of trade secrets and scarce availability of comparable licenses to determine a reasonable royalty.

Calculating damages in their exact amount could be a very burdensome task for the trade secret holder. Thus, courts and legislators have introduced some mechanisms that can help trade secret holders by easing that burden.

The laws in some countries explicitly provide guidance for determination of damages. In addition, a few countries provide a fixed range of amount of damages for trade secret misappropriation cases in certain circumstances, for example, if neither actual loss by the trade secret holder nor the misappropriator's profits are available.

Restitutionary damages

The purpose of restitutionary damages is to reverse the unjust enrichment of the misappropriator at the expense of the injured party. The damage is therefore generally calculated by looking at the benefit of the misappropriator and not the loss of the trade secret holder/injured party.

One of the difficult questions to be addressed case by case is that where only a part of the product or service of the misappropriator is related to the trade secret, what portion of the misappropriator's profits should be calculated as the unjust enrichment.

Example of restitutionary damages

In an Australian case, a former employee provided information to another company as a paid consultant using the former employer's trade secret. The court considered that the former employee who breached the confidentiality agreement with the former employer made profits both from the breach of contract and because of their own efforts and know-how. Thus, the portion of the former employee's profits were calculated accordingly to determine the restitutionary damages.

Source: See Federal Court of Australia, Bluescope Steel Ltd v Kelly (2007) 72 IPR 289.

Punitive damages

Generally, punitive damages are granted against a deliberate infringer who has behaved in a particularly egregious manner. At the court's discretion, damages that go beyond the actual damages may be awarded. Their function is to punish the misappropriators and deter them and third parties from carrying out similar actions. Punitive damages are traditionally granted in common law jurisdictions such as the United States of America and Canada, but are also available in some civil law jurisdictions such as China.

Attorney's fees and costs

In addition to damages, it is common that the successful party can recover, at least partially, the attorneys' fees and legal costs incurred in litigation. The court may typically quantify the recovery of fees and costs according to the circumstances of the case within a minimum and a maximum amount set by applicable law, depending on the complexity of the case.

Which monetary remedies are available and how they are calculated depend on the jurisdiction and the specific case. Many laws combine monetary remedies with different functions with different methods of calculation. The general principle in combining them is not to duplicate the compensation for the same harm. Where available, exemplary damages, having their own independent punitive purpose, are often granted in addition to other monetary remedies.

In litigation, the calculation of damages may be determined separately, after the issues concerning the existence of the trade secret and its misappropriation have been decided. In some countries, it is also common that the courts receive testimony from experts providing their opinion on the economic issues, helping the court to quantify and justify damages.

Case example: PPG Indus. v. Jiangsu Tie Mao Glass Co (United States of America)

In a case concerning the misappropriation of a trade secret related to a new kind of plastic for airplane windows, the U.S. Court of Appeals for the Third Circuit upheld an award of unjust enrichment damages.

The Court awarded the plaintiff the additional costs the defendant would have incurred to develop the misappropriated technology without the benefit of the trade secrets. The Court of Appeals upheld the district court decision according to which research and development costs provide an appropriate measure of the defendant's unjust enrichment. The Court also upheld the lower court's exemplary damages award, doubling the monetary damages because the defendant's misappropriation was willful and malicious.

The Court also granted injunctive relief, noting that "[t]he damages and permanent injunction covered entirely separate periods of past and potential future use of misappropriated trade secrets."

Source: See PPG Indus. v Jiangsu Tie Mao Glass Co., 47 F.4th 156 (3d Cir. 2022)

3.3 Other remedies

In addition to injunctions and monetary remedies, courts and legislations generally provide additional remedies to protect the trade secrets. They include:

- Destruction, or return to the trade secret holder, of any document, object, material, substance or electronic file containing or embodying the trade secret (examples: Canada, China, India and Singapore).
- Measures regarding infringing goods, including: (a) removing from the market; (b) destruction; and (c) seizures (examples of jurisdictions that adopted one or more of the listed measures: Brazil, India, Japan, Russian Federation, South Africa and the United Kingdom as well as EU member states implementing the EU Trade Secret Directive).
- Destruction or removal of the materials and/or equipment (predominantly) used to produce infringing goods (examples: Italy, Japan and Russian Federation).
- Assignment of ownership of the infringing goods and/or the means uniquely designed to manufacture the infringing goods or implement the infringing method (example: Italy).
- Publication of the judgment, in full or in part, with due preservation of confidentiality,[5] or other measures for the dissemination of the information concerning the decision (for example, see the EU Trade Secret Directive). Generally, publications are made in newspapers or online, in specialized magazines in the relevant industry. A court may order a publication about the court's ruling on the misappropriator's website.[6]

Some of these remedies can also be obtained in the form of provisional measures, such as the seizure or delivering up of the suspected infringing goods, with the aim to preserve the *status quo* during the time needed to reach a full decision on the merits.

The availability and applicability of those most common remedies depend on national legislation and case law. In addition, special additional remedies may be available. For example, the federal U.S. trade secret law allows a court to prevent the further dissemination of trade secrets with *ex parte* seizures.[7] The peculiarity is that the property that may be seized is potentially quite broad and not limited to the infringing goods, as is typically the case for intellectual property seizures. Another example is found in the law of the Russian Federation, where the court may direct that a legal entity be dissolved, if the entity repeatedly violates intellectual property rights.[8]

3.4 Alternative dispute resolution

General consideration on ADR mechanisms

As an alternative to litigation, parties to disputes involving trade secrets may attempt to solve them amicably through direct negotiation or have recourse to alternative dispute resolution (ADR) mechanisms, such as mediation or arbitration, in which a third party assists in or directs resolution.

Referral to ADR is consensual and can be made at different times through:

- an ADR contract clause for the submission of future disputes under a particular contract (e.g., employment contract or R&D contract), or
- a submission agreement for existing disputes, including those referred by courts.[9]

5 See Section 6.4, below.
6 See, for example, Salt Ship Design AS v Prysmian Powerlink SRL [2021] EWHC 3583, where a UK court ordered the defendant to display on its website, for six months, a statement declaring that the court had ruled that the defendant had misused the claimant's confidential information, with a link to the full judgment.
7 Claudia Ray, Joseph Loy, Miriam Kontoh and Andrew (Keum Yong) Lee (2024). USA: Law and Practice. In Chambers Global Practice Guides, Trade Secrets 2024, p. 229. https://chambers.com/downloads/gpg/1014/trade_secrets_2024.pdf.
8 Art. 1253 of the Civil Code of the Russian Federation (Russian Federation). English translation available at WIPO Lex Database. https://www.wipo.int/wipolex/en/main/legislation.
9 The website of the WIPO Arbitration and Mediation Center (https://www.wipo.int/amc/en/) provides information about benefits of ADR mechanisms and various services offered by the Center. It also makes available model contract clauses and submission agreements in several languages to facilitate referral of intellectual property and technology disputes, including trade secrets, to WIPO ADR procedures. See also the Annex to this Guide (A List of Reference Materials).

As time- and cost-efficient alternatives to litigation, ADR options can offer significant advantages in the context of disputes involving trade secrets. ADR gives parties flexibilities to customize their dispute resolution process in a single and neutral forum. Another key advantage of ADR is confidentiality of the dispute resolution process and its outcome, which is of fundamental importance where commercial reputation and trade secrets are involved.

Mediation

Mediation is an ADR mechanism where a neutral third party, the mediator, assists the parties in reaching a mutually satisfactory settlement of their dispute, based on the parties' respective interests.[10] Any settlement can be enforced as a contract or, depending on the jurisdiction, even as a court order.

In addition to being particularly time- and cost-efficient, mediation offers many other advantages to parties involved in trade secret disputes. It is a non-binding and interest-based procedure. It gives parties control over the process and its outcome, as there is only a binding result if parties agree to it. Mediation provides a high control of confidentiality and parties cannot be forced to file or disclose documents. Further, the parties can engage themselves to not disclose, even as evidence in future judicial or arbitral proceedings, any information or document exchanged.

Arbitration

In arbitration, the parties stipulate an agreement wherein they submit a dispute to arbitrator(s) often specialized in the relevant field, who make a binding decision on a dispute. Unlike mediation, once the parties have validly agreed to submit the dispute to arbitration, neither party can unilaterally withdraw from the procedure, and the final award of the arbitrator(s) is binding. Therefore, court options are normally foreclosed when arbitration is agreed. Also, the arbitral decision is not based on the parties' respective interests, but on the parties' respective rights and obligations as determined by the arbitrator(s). The arbitration aims to resolve the dispute according to the applicable law, and not to settle the case in a manner agreeable for all the parties.

Arbitration can have several advantages compared to litigation: (i) an arbitration procedure can be flexible - the arbitrator(s), the applicable law, the language of the procedure and the seat of arbitration are typically selected by the parties; (ii) if the unsuccessful party fails to voluntarily comply with the award, the decision can be enforced in most parts of the world pursuant to the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958; and (iii) costs may be lower under a single arbitration procedure, compared to litigating complex cross-border disputes in various parallel national court proceedings.

Whether arbitration is a better choice than litigation depends both on the specific circumstances of the case and where a lawsuit could be filed. In some instances, trade secret holders might come to the conclusion that relief that can be obtained through judicial provisional measures to protect its rights or to preserve evidence, such as *ex parte* search or seizure orders, outweighs the benefits of arbitration.

4. How to build a strong trade secret case

If a trade secret holder or a licensee (where applicable) decided to start litigation, there are several issues that need to be looked at before taking action.

10 According to the statistics published by WIPO, over 70 percent of the mediation procedures administered by the WIPO Arbitration and Mediation Center result in a settlement agreement. See WIPO Caseload Summary, available at: https://www.wipo.int/amc/en/center/caseload.html.

4.1 Choosing defendants

An important choice to make is whom to sue. The action will likely be directed primarily against the direct misappriopriator. However, under certain circumstances, it could be appropriate to file the action against additional parties.[11]

For example, if a former employee who had left to work for a competitor unlawfully acquired, distributed or used the trade secret of the former employer, it could be appropriate to sue the competitor who hired the former employee. The legal basis of the action would be the direct or indirect liability of the new employer, according to the circumstances of the case and the applicable law. One can imagine different scenarios.

- If the new employer knew about the misappropriation in advance, the employer would likely be directly liable for the misappropriation, along with the new employee who performed the wrongful action (such as unlawfully using the trade secret or sharing the trade secrets with colleagues at the new employer).
- Similarly, the new employer could be held liable if its employee is induced or misguided by the new employer to engage in an act of misappropriation.
- In general, the new employer could still be liable if it knows, or it should have known with the diligence and care normally expected, that the employee committed trade secret misappropriation.
- If the new employer, even if it has taken proper due diligence and care, did not known that the trade secret of the former employer was misappropriated by its employee, the new employer generally becomes liable when it becomes aware of such misappropriation and nevertheless continues to use or disclose the information.
- There may be vicarious liability rules due to the special relationship of the employer with the employee, depending on general tort law, labor law or eventually unfair competition law, which vary among jurisdictions.

Once unlawfully acquired by a third party, trade secret information can be passed easily from one person to another, without any indication that the information belongs to the legitimate trade secret holder. Therefore, there can be recipients who innocently believe that they lawfully receive, use or distribute that information. Trade secret holders, however, generally cannot claim damages for misappropriation against such innocent recipients before they know (or should have known) of the misappropriation. Consequently, the trade secret holder may decide to also sue innocent recipients, since notification of the initial complaint would make them aware of, and henceforth liable for, any subsequent act of use or disclosure of the trade secret. To be on the safe side, however, whether the applicable law provides any conditions or requirements relating to pre-suit action of the claimant should first be checked.

4.2 Burden of proof

General principles

A widespread civil procedure rule in almost all legal systems is that the burden of proof is usually on the person who makes a claim. This generally applies also in trade secret cases. The subject matter of proof obviously depends on the legal claims put forward in the trade secret misappropriation proceedings.

For example, if contractual confidentiality obligations are enforced, the plaintiff shall provide evidence of a valid binding contract and breach of the contract. If unfair competition claims are made, the plaintiff shall generally provide evidence that the parties are competitors and that there is an act amounting to unfair competition. If the action is based on tort law, the plaintiff shall generally prove the defendant's willful misconduct or negligence.

Regarding trade secret misappropriation cases, in general, the trade secret holder must:

- show its entitlement to sue (see 2.4)

11 See Section 2.1 regarding misappropriation of trade secrets.

- identify the trade secret for which it is seeking protection; this is a delicate part of the claimant's pleading because courts generally require sufficient specificity, otherwise the court could dismiss the case
- prove that the information qualifies as a trade secret, which means that all the legal requirements for trade secret protection are met
- prove the misappropriation, and
- if monetary remedies are sought, the trade secret holder shall prove the amount of the damages suffered or the profits of the defendants (see 4.3).

The next paragraphs focus on the third and the fourth points, while the other points have already been discussed.

Proving that the information qualifies as trade secret

Patents, for example, are granted by an administrative authority, which examines compliance of the claimed invention with applicable legal requirements. However, since trade secret protection is not subject to any registration, there is no assumption that the information alleged by its holder meets the criteria for trade secret protection. Thus, the trade secret holder generally bears the burden to show that the legal requirements for trade secret protection[12] are met.

Proving "secrecy"

It is almost impossible to prove negative facts, such as whether the information is "not" generally known or readily accessible among persons within the relevant circles. Consequently, trade secret holders generally demonstrate the confidentiality and security measures that they have taken to maintain secrecy and explain why the information is deemed not generally known (for example, by showing competitors' activities and market trends) or readily accessible.

Depending on the facts of the case and applicable law, examples of the factors that may be considered to prove secrecy include:

- the extent to which the information is known outside your business
- the extent to which the information is known to your employees and others involved in the business
- the level of the engineering or technological development and the complexity of the information
- the investment made to create the information or the difficulty that competitors can face in properly acquiring the information.

Proving commercial value due to secrecy

The link between the commercial value of the information and its secrecy may be established, for example, when the unlawful acquisition, use or disclosure is likely to harm the trade secret holder because it undermines the holder's business or financial interests or its strategic and competitive position in the market. There are various ways to prove the commercial value due to secrecy. For example:

- the savings or the competitive advantage of the trade secret holder vis-à-vis its competitors
- the time and money invested by the trade secret holder in obtaining and developing the information
- the investment that would be incurred by a third-party competitor if it were to acquire or duplicate the information.

The fact that competitors are trying to obtain the information (through licensing, for example) may indirectly demonstrate the commercial value of the trade secret.

12 See Part III: Basics of trade secret protection for the three criteria to be met for information to be trade secrets.

Proving "reasonable steps"

It is advisable for the trade secret holder to show in court all the different measures and steps implemented to maintain the secrecy of the information.

Although what is "reasonable" necessarily depends on the unique circumstances of the trade secret holder, the evidence to prove reasonable steps could include:

- internal policies and guidelines for the management of confidential information
- non-disclosure agreements (NDAs) and contracts including confidentiality clauses signed by employees, vendors, suppliers, external partners etc.
- adequate security measures, including diligent management of information and communication systems and physical controls, and
- affidavits and witnesses testifying to the implementation of any of the above or of any additional protection.[13]

Proving the misappropriation of the trade secret

Proving the misappropriation means proving that the defendant acquired, disclosed or used the trade secret with unlawful, improper or dishonest means, according to different national applicable standards (see also Section 2.1).

In this context, the trade secret holder must prove:

- the misappropriation specifically concerned its trade secrets – the misappropriated information should be the same as the enforced trade secret, and
- the unlawful, improper or dishonest means used by the misappropriator, for example, breach of confidentiality obligations, breach of confidentiality duties arising from special relationships (e.g., employer–employee relationship), industrial espionage, hacking, inducement to breach, coercion etc.

Generally, proving actual or threatened misappropriation is sufficient. Eventually, proof of harm to the trade secret holder is necessary for claiming damage compensation.

When a third party has used or disclosed the trade secret information, in general, trade secret holders do not need to prove that the information originated from the trade secret holder, but they still may need to prove that they are the legitimate holder of the information.

Particular challenges for proving misappropriation

Misappropriators are often aware that their actions are improper, and thus try not to leave any evidence of their unlawful behavior. In addition, if the purpose of misappropriation is to obtain the valuable trade secrets of a competitor, a misappropriator will try to keep such trade secret information tightly within his/her company and use it secretly. Thus, in general, it is difficult for trade secret holders to obtain direct evidence proving the key facts of misappropriation. As will be explained in the next subsection, certain measures and procedural rules to obtain additional information and evidence from another party may help trade secret holders to collect evidence.

In trade secret cases, indirect or circumstantial evidence plays a major role in proving the misappropriation. Although such evidence does not directly prove the key fact, they establish facts from which a reasonable person can make an inference that the key fact existed. Admissible "inference" must be distinguished from impermissible "speculation."

According to some legal systems, indirect evidence can build a presumption that the key fact happened, and shift the burden of proof on the defendant.

13 See Part IV: Trade secret management, in particular 2.3 regarding operational and contractual protection measures.

Example of reversed burden of proof

According to Article 32 of the Anti-Unfair Competition Law of China, the alleged infringer of the trade secret shall prove the absence of infringement if a lawful holder of the trade secret submits *prima facie* evidence to prove that it has taken confidentiality measures for the claimed trade secret, and to reasonably indicate that the trade secret has been infringed upon, and submits any of the following evidence:

- evidence indicating that the alleged infringer had the method or opportunity to obtain the trade secret, and the information it used is substantially the same with such trade secret evidence indicating that the trade secret has been disclosed or used, or is at risk of disclosure or use, by the alleged infringer, or
- other evidence indicating that the trade secret has been infringed upon by the alleged infringer.

To conclude, indirect evidence or, better, a mix of direct and indirect evidence, can still provide the court with a sufficiently convincing picture of the misappropriation depending on the facts of the case and applicable law.

Case example: Tradingall Electronic S.L./Aplicaciones Electronicas y De Radiofrecuencia S.L: SAP BA 187/2019 (February 19, 2019)

The case concerns the alleged misappropriation of software source code, which was allegedly protected as a trade secret.

On appeal, the alleged misappropriator claimed that the trade secret holder did not prove that it had accessed to the source code.

The Court of Appeal of Barcelona however found that both parties' products and catalogues were (almost) identical. According to experts, the high number of coincidences between the two products could not have been accidental.

Therefore, to the Appeal Court, it is not necessary to find out whether there has been actual acquisition of the software in order to assess whether there has been an infringement of trade secrets.

In other words, the Appeal Court did not require direct evidence of access to prove that the trade secret in question had been illegally acquired. Instead, unlawful trade secret acquisition was assumed due to the extreme similarity between the products that resulted from the information.

Note: For a more detailed explanation of the case, see: European Union Intellectual Property Office (2023). Trade Secrets Litigation Trends in the EU. European Union Intellectual Property Office, pp. 148–149. Available at: https://data.europa.eu/doi/10.2814/565721.

4.3 Collecting evidence for proceedings

It is best to collect relevant evidence as early as possible and before alerting the misappropriator through a warning notice or a cease-and-desist letter, since after such notice, the misappropriator could conceal or destroy evidence of the misappropriation.

To make sure that collected evidence is admissible in court, it must be collected according to applicable rules of procedure and in compliance with other areas of law (such as privacy law or labor law). For instance, tracking and monitoring employees' activities can be done in certain jurisdictions only and to a certain extent, in compliance with limitations set by labor and privacy laws.

Also, best practices and standards in digital forensics should be followed.

During or in preparation for court proceedings, the trade secret holder can usually rely on some measures and procedural rules to obtain additional information and evidence to strengthen its case. These measures generally seek to strike a balance between the interest of the trade secret holder to have access to evidence and the interests of the alleged misappropriator to maintain the secrecy of its own valuable information. While they differ from one country or region to another, in principle, two types of measures may be available: provisional measures for preserving evidence and discovery proceedings.

Provisional measures for preserving evidence

In many jurisdictions, courts have the authority, even before commencement of the proceedings on the merits, to order provisional measures for preserving evidence, provided that certain conditions are met. Generally, these conditions require the claimant to provide at least *prima facie* evidence of the case.

Discovery proceedings

Pre-trial discovery in common law countries

Pre-trial discovery is the formal process of exchanging information between the parties about the evidence the parties will present at trial. The rationale is to ensure that the parties have mutual knowledge and access to all relevant facts that are essential to litigation ahead of the trial. Common law countries such as Australia, India, and the United States of America tend to favor some amount of voluntary pre-trial disclosure between the parties, outside of the direction and compulsion of the court.

The United States of America, in particular, provides for very extensive pre-trial discovery, both under state and federal law, including documentary review, written questions and answers, pre-trial depositions under oath, requests for the productions of documents, and inspections.

Complex issues of international comity may arise when evidence supporting the parties' claims and defense in a trade secret case is located outside the country where the litigation is pending, and therefore cross-border discovery is needed.[14]

Court orders to provide documents in civil law countries

In civil law countries, in principle, the party bearing the burden of proof is responsible for collecting evidence to support its case and may obtain only limited documentary evidence through and under the supervision of the court.

However, a limited form of discovery may be available. Generally, a party needs to show that certain documents are relevant for the case and that the other party, or a third party, holds such documents and request the court to order a party to submit those documents. Such orders typically concern not only material showing the misappropriation, but also business records, banking, financial or commercial documents, which are under the control of the alleged misappropriator and are useful to determine the extent of the misappropriation or its unlawful profits.

Finally, parties can generally rely on ordinary means of evidence, such as hearing witnesses, experts and third party examination.

In many countries, more evidence could be gathered through criminal proceedings, since the prosecution authority generally has extensive powers to search and seize evidence (see Section

14 See The Sedona Conference, Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases, The Sedona Conference Working Group Series, Public Comment Version (2021); The Sedona Conference, Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases ("Stage Two"), The Sedona Conference Working Group Series, Public Comment Version (2023). Both available at: https://thesedonaconference.org/.

8.1). In a limited number of countries, a similar goal can be pursued also through administrative authorities (see Section 8.2).

5. Defense against trade secret misappropriation claims

In response to the accusation of the trade secret holder, the alleged misappropriator should be given the opportunity to defend itself against the accusation. In general, there are two main lines of defense:

- the information is not a trade secret, and
- acquisition, use or disclosure of the trade secret by the alleged misappropriator was accomplished without unlawful, improper or dishonest means.

5.1 Non-existence of trade secret

The first and most common defense in a trade secret misappropriation case is that the information for which protection is sought does not qualify as a trade secret. As discussed, generally the trade secret holder needs to prove eligibility of the information as a trade secret. The defendant typically tries to rebut the trade secret holder's claim by proving that:

- the information had already fallen into the public domain before the alleged misappropriation, and it is generally known among persons in interested circles
- the information was readily accessible to persons within the interested circles. For example, the persons in the interested circle could collect raw data from the Internet, and with the assistance of a computer, could extract the alleged trade secret information with a trivial effort, or
- the trade secret holder had not taken reasonable steps to keep the information secret. For example, the defendant may demonstrate that standard protection measures taken by competitors in the market are usually higher than those taken by the trade secret holder, or the trade secret holder had not taken reasonable diligence to update its IT systems or close security loopholes.

5.2 No trade secret misappropriation occurred and exemptions from liability

A second common defense against misappropriation claims is that unlawful, improper or dishonest acquisition, use or disclosure of the trade secret has never occurred. This is mainly a matter of facts and evidence.

Authorized access and use defense

The defendant may argue that it acquired, used or disclosed the trade secret in a lawful, proper or honest manner, and hence, no misappropriation occurred.

For example, if the trade secret information was obtained with an NDA defining the contractual boundaries of the authorized use of the information, the defendant may provide evidence that its use of the information was inside the boundaries of the NDA, and hence it did not misappropriate the trade secret.

Bona fide defense

As explained in Section 2.1 above, if third parties acquired the trade secret information in good faith, they may be entitled to use or disclose such information lawfully, depending on applicable law. Therefore, the defendant may bring the so-called bona fide defense, if applicable.

Independent discovery defense

The defendant may assert that it had independently discovered, and subsequently used, the same trade secret information protected by the trade secret holder.

To successfully raise this defense, keeping track of the status and the progress of research and development activities and other business activities is important to show that the information was acquired autonomously.

Reverse engineering defense

The defendant could claim that the trade secret was obtained through reverse engineering, which is generally not considered a trade secret misappropriation unless a valid and enforceable contract forbids reverse engineering.

To bring the reverse engineering defense, the defendant needs to prove that it did in fact acquire the information through its own reverse engineering, not merely that it would have been possible to do so. Therefore, similar to the independent discovery defense, it is advisable to record the reverse engineering operations in a way that it can be used as evidence.

Employee's skills and experiences

To protect employees' mobility, it is widely understood that departing employees are free to use their general knowledge, skills and experience acquired in their normal course of employment.

In practical terms, it can be difficult to distinguish the employees' general knowledge, skills and experience from the former employer's trade secrets. To make such a distinction, courts have adopted various approaches, considering, for example:

- whether the employee took documents and information in a written or some other tangible form, or whether the employee merely remembered it
- whether the employee's knowledge and skills were acquired before or while working for the employer who claims such knowledge and skills as a trade secret
- whether the employee's knowledge and skills are general to the particular industry or trade, or whether they are specific to the employer's particular business
- whether the employee has acquired specific expertise, techniques or know-how in using an employer's trade secret during his or her employment
- whether the employer used secrecy measures making it sufficiently clear to employees and third parties that certain information is considered a trade secret and proprietary to the company.

Public interest and whistleblower defense

In special cases, and according to national/regional laws, the defendant may be able to argue that its act of acquisition, use or disclosure of the trade secret is excluded from liability due to the fact that such action was made to further the public interest, such as public health or safety. For example, Article 1472 pf the Civil Code of Québec, Canada, states "A person may free himself from his liability for injury caused to another as a result of the disclosure of a trade secret by proving that considerations of general interest prevailed over keeping the secret and, particularly, that its disclosure was justified for reasons of public health or safety."[15]

Similarly, in countries/regions such as the United States of America or EU member states, the law allows for disclosure of trade secrets when it is necessary to act in the general public interest and reveal misconduct, wrongdoing or illegal activities. Under these specific and limited circumstances, a defendant may raise this defense providing evidence for the act of whistleblowing.

Workers' rights to information

The EU Trade Secret Directive[16] provides a safe harbor when trade secret disclosure occurs as part of the legitimate exercise by workers' representatives in the exercise of their functions, or

15 In the United Kingdom, according to Regulations 12(2) and 15(1) of the Trade Secrets (Enforcement, etc.) Regulations 2018, a court must take into account certain specific circumstances, including public interest and safeguard of fundamental rights, in assessing the proportionality.
16 Article 3(1)(c) of the EU Trade Secret Directive (EU) 2016/943.

by workers engaged in legitimate consultation with their representatives. Such exception seeks to prevent trade secret protection from undermining workers' rights to obtain assistance from representatives during negotiations with the management.

6. Preservation of trade secret during court proceedings

In many countries, it is common that court hearings are public, and judgments are usually published. The transparency and accessibility of court proceedings are cornerstones of the rights to justice. However, in trade secret cases, a trade secret holder generally needs to identify its trade secrets and to disclose them in the court files to support its claims.

Thus, measures that preserve confidentiality of trade secrets during court proceedings are necessary to avoid jeopardizing trade secret protection. On the other hand, the defendants sued for trade secret misappropriation need access to the alleged trade secrets to defend themselves properly. For these reasons, legislators and courts of many countries provide and apply measures to preserve confidentiality of trade secrets, which aim to strike a balance between the competing interests of the parties as well as the general public.

These measures to preserve confidentiality during the proceedings ultimately depend on applicable national procedural law. Nevertheless, there are some widely accepted measures in various jurisdictions.

6.1 Access restrictions

Courts typically restrict the access to proceedings and court's files that are likely to contain and describe trade secrets. The restriction can be ordered for access to:

- the (parts of) documents containing (alleged) trade secrets
- the (parts of) hearings and the minutes of the hearing where (alleged) trade secrets are likely to be disclosed. In some countries, courts may hold in camera proceedings (i.e., proceedings under legal secrecy in, for example, judge's chambers instead of in open court).

6.2 Protective confidentiality orders

Courts typically impose duties of confidentiality on anyone who participates in the proceedings or has access to the documents of the proceedings, including judges, lawyers, witnesses and court personnel. Often, the imposition of such duties requires a specific court order, usually upon the request of the interested party. However, in some countries, such as Singapore, the implicit duty of confidentiality applies under certain circumstances.

The duty of confidentiality generally lasts until the order is removed, the final decision that the alleged trade secret does not qualify as trade secret is established, or until the information no longer meets the criteria for trade secret protection.

6.3 Confidentiality clubs

The court may decide to restrict access to trade secrets or related information to a limited number of participants to the proceedings, creating a so-called "confidentiality club" or "confidentiality ring" (for example, in Canada, India, Singapore, Switzerland, the United States of America and according to the EU Trade Secret Directive).

While protective orders impose general duties of confidentiality on all the participants in the proceedings and those who have access to the court's files, the *confidentiality club orders* restrict access to specific documents to specific individuals. In addition, a *confidentiality club order* typically points out how the documents should be handled by the members of the club, for example, if and how documents may be copied or where the documents may be viewed.

The most debated issue regarding confidentiality clubs concerns the individuals included in the club. Very restrictive confidentiality club orders are *attorneys-eyes-only* or *expert-eyes-only*. However, excluding the parties and their representatives from the club could create frictions

with the fair trial and adversarial principles, since defendants may complain that the prohibition puts them in a weak position without adequate defensive means. A court needs to keep the balance between rights and interests of both parties depending on the concrete circumstances of the case.

6.4 Non-disclosure of trade secrets in judgments

In many countries, a redacted version of the judgment, without disclosure of the trade secret information, is published by the courts. An unredacted version of the judgment will be made available to the parties only, together with protective orders not to disclose its content.

7. Cross-border issues

Cross-border litigation relating to trade secret disputes is not very common.[17] However, as trade secrets are not subject to any form of registration, they can theoretically be immediately protected in any jurisdiction where they meet the conditions for legal protection.

Information in general and digital information in particular crosses national borders easily. Trade secrets may be unlawfully acquired in one country by a misappropriator located in another country, and used and publicly disclosed by other parties in yet other countries, without any authorization of the trade secret holder.

In such cross-border disputes, determining jurisdiction and applicable law becomes a more important question, compared to those cases where the parties reside, and the misappropriation occurred, in the same jurisdiction. In addition, the extraterritorial reach of the remedies granted by courts has an impact on both parties.

General rules and doctrines on these issues, also applicable to trade secret disputes, are covered by private international laws, and have been developed at the international, regional and national levels.[18]

7.1 Jurisdiction

Where the trade secret holder can file a suit is a matter of jurisdiction. Jurisdiction is the authority of a court to hear and decide on the merits of the case. Generally, each country sets its own jurisdiction rules, and courts themselves should decide on their own jurisdiction. Jurisdiction rules can also be regulated by international conventions or regional legislative acts such as the EU Regulations.

Courts generally rely on the so-called “connecting factors” to establish their competence to decide a case. As the national jurisdiction rules and the related case law differ, the assessment must be done on a jurisdiction-by-jurisdiction basis. Additionally, the legal basis of the protection sought (for example, tort or contract law) can affect applicable jurisdiction rules.

Despite the complexity of the topic, a few recurring rules that ground jurisdiction on similar connecting factors can be identified in the different legal systems:

Domicile of the defendant (or similar territorial connecting factors)

Many laws provide that the defendant can be sued in the country of its domicile, permanent home, habitual residence or similar territorial connecting factor. Regarding companies, connecting factors that ground jurisdiction are generally the place of the registered office, principal office or business office.

17 Based on a data set of 700 trade secret-related decisions in the EU, all parties were based in the same EU member state in 86 percent of cases. See Trade Secrets Litigation Trends in the EU, European Union Intellectual Property Office, 2023, p. 29. Available at: https://data.europa.eu/doi/10.2814/565721.

18 See, for example, Bennett, A. and S. Granata (2019). When Private International Law Meets Intellectual Property Law - A Guide for Judges. WIPO Publication No. 1053. https://www.wipo.int/publications/en/details.jsp?id=4465&plang=EN.

Domicile of the claimant

Less frequently, national laws ground jurisdiction on the base of the domicile of the claimant.

Forum commissi delicti and/or forum damni

The law generally provides jurisdiction if there is a territorial connection between the country and the unlawful activities.

Nationality of the defendant

According to other approaches, the place where the illicit conduct was carried out (place of action) and/or the place where the damages occurred or may have occurred (place of effect) are relevant.

A few countries' laws also look at the nationality of the defendant to determine jurisdiction.

Forum (non) conveniens

Mainly in common law countries, courts apply the forum (non) conveniens doctrine, which allows courts having jurisdiction over a case to stay or dismiss the case upon a determination that another court where the case might have been brought is a more appropriate forum for the interests of all the parties and the ends of justice.

7.2 Applicable law

After the determination of its jurisdiction, a court needs to determine the applicable law. A court may be deemed to have the jurisdiction to decide the case, but according to foreign law.

The applicable law may be determined under national law, international conventions or regional legislative acts such as EU Regulations. Different connecting factors according to private international law apply to breach of contract, tort law, unfair competition law and intellectual property. Therefore, the court will generally need to analyze the nature of the claim.

In essence, determination of the applicable law involves choosing between different bodies of law (contract law, tort law etc.), consideration of the national law of the court (particularly mandatory rules), connecting factors and choice of law principles and the applicable law agreed between the parties, if any.

7.3 Extraterritorial reach of the remedies

When acts of misappropriation, or different fractions of the same conduct, are carried out in different countries, questions may arise as to whether the court with jurisdiction can also address the acts carried out in another jurisdiction, i.e., extraterritorial acts, and whether the court can issue cross-border measures that concern or affect extraterritorial activities.

If the extraterritorial trade secret misappropriation occurs within a contractual context, the breach will largely be governed by the contract. Outside the contractual context, the principle of territoriality is generally applied – at least as a starting point – to trade secrets.[19] There seem to be tendencies and cases in which courts in different jurisdictions may assess extraterritorial misappropriation of trade secret and issue cross-border remedies, such as injunctions and damage awards.[20]

19 The Sedona Conference, Framework for Analysis on Trade Secret Issues Across International Borders, 23 Sedona Conf. J. 909 (2022), p. 951. Available at: https://thesedonaconference.org/publications.

20 For example, Motorola Solutions, Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150 (N.D. Ill. 2020) allowed the recovery of the defendants' profits on the sale of products incorporating the misappropriated trade secrets outside of the United States of America. See also Kappes K. and L.Laguna (2021), The Defend Trade Secrets Act and Extraterritoriality, American Bar Association. https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/articles/2021/dftsa-extraterritoriality/.

Even in cases in which a court may decide on misappropriations abroad and issue cross-border measures, the real effectiveness of such measures will largely depend on their recognition and enforcement. They are often regulated through international judicial cooperation mechanisms.

8. Criminal and administrative enforcement of trade secrets: an overview

In general, civil proceedings are the most common proceedings sought in case of trade secret misappropriation. According to a recent study, in the EU, the vast majority of proceedings are categorized as "civil cases" (89%), with a minority categorized as "administrative cases" (5%) or "criminal cases" (6%).[21] Although the absolute number of criminal cases is small, according to the 2024 annual report published by the Japanese National Police Agency, the number of arrests relating to trade secret crimes in Japan has been rapidly increasing in recent years.

8.1 Criminal enforcement

In many countries, criminal law offers additional protection to trade secret holders. Often, availability of criminal sanctions regarding trade secret misappropriation is limited to the most serious conduct, and the punishment differs according to the seriousness of the violation, reaching from a fine to months/years of imprisonment. In some countries, the punishment with a higher penalty may be applied if misappropriation was carried out with the intention of benefiting a foreign government. In some other countries, more severe punishment applies if a misappropriator intended to use the trade secrets in a foreign country or he/she committed the unlawful acquisition or disclosure of the trade secret, knowing that it would be used in a foreign country.

In general, criminal punishments have a deterrent effect against trade secret misappropriation. In some countries, such as Australia, trade secret misappropriation is not a crime. However, such misappropriation is usually carried out with means that are subject to criminal sanctions, for example, theft, fraud, coercion or electronic intrusion. Therefore, trade secret holders still have, to a limited extent, recourse to criminal proceedings in those countries.

Criminal proceedings, depending on national laws, can be pursued *ex officio* (i.e., on initiative of the prosecuting authority) or subject to a criminal complaint filed by the victim, or both. In any case, the trade secret holder can generally provide "hints" to the prosecuting authority about the trade secret misappropriation. However, once a criminal case is open, the public authorities might take full control of the investigations and the proceedings.

Civil law and criminal law proceedings are often raised in different fora and do not necessarily influence each other, since the two proceedings and available remedies are separate and independent from each other. However, depending on national/regional rules of procedure, what is established in criminal proceedings can be binding on civil proceedings to some extent, or at least be relevant in the context of civil proceedings.

Advantages and disadvantages of criminal proceedings

From a strategical point of view, enforcing trade secrets through criminal proceedings could have both advantages and disadvantages. It can be easier to obtain evidence in criminal proceedings, since public authorities generally have broader investigative power. If the national rules allow the use of evidence collected in criminal proceedings for civil proceedings, requesting criminal proceedings can be beneficial for the trade secret holder, who still needs evidence for civil proceedings.

However, once the criminal action is started upon the request of a party, public officials are in charge of the proceedings. Thus, a trade secret holder has generally only limited control over the investigation, the development of the case and its timeline. In addition, depending on the

21 Trade Secrets Litigation Trends in the EU. European Union Intellectual Property Office, 2023, p. 24. https://data.europa.eu/doi/10.2814/565721.

national rules of procedure, the prosecution of a civil case may be delayed pending the criminal proceedings. More importantly, if trade secret holders have any willingness to settle the case amicably, pursuing criminal proceedings can eliminate those settlement options.

8.2 Administrative enforcement

A limited number of countries provide for enforcement of trade secrets by administrative procedures. In general, administrative proceedings are reportedly rarely used.

In China,[22] a trade secret holder may file an administrative complaint with the local Administration for Market Regulation, which has the power to investigate trade secret misappropriations. The local Administration can order the misappropriator to cease the misappropriation, confiscate any illegal profits and impose fines.

In the Republic of Korea, trade secret holders may file a request with the Korea Trade Commission for a preliminary injunction to prohibit or prevent international unfair trade practices. They may also seek other corrective measures, including:

- suspending the import, export, sale or manufacture of the infringing goods
- banning the landing of such goods
- making corrective advertising
- publishing the fact of receiving a corrective order from the Trade Commission, or
- other necessary measures to correct unfair international trade practices.[23]

In the United States of America, when an act of trade secret misappropriation occurs outside the country, the trade secret holder may seek relief through an action brought before the International Trade Commission (ITC). ITC is a federal agency that adjudicates cases involving imports that allegedly infringe intellectual property rights, including trade secrets. It has the authority to exclude imports, if it finds anti-competitive practices and unfair acts in the importation of articles.

9 Trade secret litigation in practice

Since the value of trade secrets derives from their secrecy, many unique challenges arise where trade secret holders detect potential trade secret leakage or misappropriation. Navigating trade secret litigation is complex. Trade secret holders need to make critical decisions to prevent, or minimize, damages caused by misappropriation or leakage. Built on the Case Example of "Serve Machine 1100" in Part IV, the following story shows an example of how a trade secret holder may handle a trade secret dispute.

Case example: "The Serve Machine 1100" – Trade secret litigation

The Super Tennis Racket Company is one of the biggest tennis rackets producers worldwide. Its current business success greatly owes to an innovative manufacturing machine named "The Serve Machine 1100". The most valuable features of that machine have been protected as trade secrets.

One day, Anna, who had been a member of the R&D team of the Company that developed the "The Serve Machine 1100" but was working on another project at that time, left the Company. A few months after her departure, it turned out that:

- Anna lied at her exit interview, concealing the identity of her new employer who is a competitor named The Bad Player
- During her last days of work, Anna had opened an impressive number of documents related

22 Articles 13 and 16 of the Law of the People's Republic of China Against Unfair Competition (as amended up to April 23, 2019). English translation available at the WIPO Lex Database. https://www.wipo.int/wipolex/en/main/legislation.
23 Articles 7(2) and 10(1) of the Act on the Investigation of Unfair International Trade Practices and Remedy Against Injury to Industry (Republic of Korea). English translation available at: https://elaw.klri.re.kr.

to the "The Serve Machine 1100" on her business laptop, only for a few seconds per each document. Her colleague saw Anna taking photos of her desktop screen with her smartphone.

Although the colleague could not see what was on her screen, from the circumstances, The Super Tennis Racket Company strongly suspected that Anna had taken photos of the documents containing the trade secret information and had disclosed them to The Bad Player.

The Super Tennis Racket Company hired an external computer forensics expert and asked him to freeze the evidence of the operations carried out by Anna on the laptop during the last days of work at the Company so that it will have convincing evidence that can be filed in court.

Due to the need to intervene rapidly and not to alert The Bad Player and Anna, The Super Tennis Racket Company decided not to send a cease-and-desist letter to them, but proceeded directly with a lawsuit against them for trade secret misappropriation.

The events occurred in Italy. The competent court is the Court of Milan, where an intellectual property specialized division deals with trade secret cases on a regular basis.

While filing its application in Court, The Super Tennis Racket Company identified its trade secrets and asked the Court to adopt confidentiality measures to preserve their confidentiality in the proceedings. The Super Tennis Racket Company also explained to the Court why the information related to the innovative features of the "The Serve Machine 1100" would qualify trade secret protection.

In its application, The Super Tennis Racket Company asked the Court for:

- an *ex parte* provisional measure for preserving evidence held by Anna and The Bad Player, consisting of the detailed description of the information and documents misappropriated, and the materials and implements used in the production and/or distribution of the infringing products relating to the trade secrets, and
- an *ex parte* preliminary injunction against Anna and The Bad Player from using the misappropriated trade secrets and documents.

The Court granted the requested measures *ex parte*. It was persuaded *prima facie* certain features of "The Serve Machine 1100" qualified for trade secret protection. The circumstantial evidence provided by The Super Tennis Racket Company well demonstrated that the trade secret misappropriation by Anna and the Bad Player happened more likely than not. The Court was also persuaded that the requested measures should be granted on an urgent basis and *ex parte*, due to the risks related to a possible disclosure of the trade secrets by the time when a decision on the merits could be obtained and the risk of the destruction of evidence if the defendants were alerted in advance.

The Super Tennis Racket Company enforced the Court's measures. The documents of The Super Tennis Racket Company were found on Anna's smartphones and The Bad Player's data management system. In some emails, the management of The Bad Player discussed how to better exploit the information and documents provided by Anna. The Bad Player was clearly aware of the misappropriation.

The Bad Player and Anna filed their defense in court, claiming that the pieces of information allegedly misappropriated cannot be qualified as trade secrets, because they would not meet the requirements for trade secret protection. In particular, they claimed that The Super Tennis Racket Company failed to take reasonable steps to keep the information secret. Also, they argued that Anna acquired the relevant information in the fulfilment of her working duties in developing "The Serve Machine 1100" in the R&D team of The Super Tennis Racket Company, and therefore such information would be part of her general skills and experience that she is allowed to use freely.

The Court was not persuaded by the defendant's counter arguments. The Court deemed that the documents bearing the trade secret information of which Anna had systematically taken pictures during her last days of work, were not part of Anna's general skills and experiences obtained during her employment.

With regard to the reasonable steps requirement, the Court considered that The Super Tennis Racket Company successfully met the necessary standard by showing its trade secret management plan and its implementation in the Company, including various protection measures taken by the Company.

The Court confirmed the provisional measures and the preliminary injunction already granted *ex parte* against the defendants.

Anna and The Bad Player did not want to go through proceedings on the merits where they could be forced also to pay damages for the misappropriation. Therefore, they proposed The Super Tennis Racket Company to negotiate and find an amicable solution to settle the dispute.

Part VI: Trade secrets in collaborative innovation

Topics covered in this Part:

- **Particularities of trade secret management in collaborative innovation**
- **Management of trade secrets through different phases of collaboration**
- **Protection and use of trade secrets by universities**
- **Handling trade secrets in university–industry collaboration**

Many recent books and articles have stressed the importance of collaborative innovation models not only for companies' competitiveness but also for accelerating creation of innovative products for the benefit of the public at large. Collaboration between public research institutions and private companies has been encouraged in many countries with a view to facilitating practical application and commercialization of public research outputs.

In practice, collaborative research brings in researchers from two or more organizations, having the required expertise, knowledge, know-how and skills, to one project. They collectively contribute to a common goal.

Trade secrets as background IP. Oftentimes, not to share trade secret information with other collaborating researchers at all is not an option, since cross-fertilization of shared knowledge and know-how is key for success in collaboration. Thus, if trade secret information is considered relevant to the collaboration, trade secret holders may ask themselves how and under what conditions their trade secrets should be shared with other collaborators so that both the value of the trade secrets for the company and successful outputs from the collaborative process will be maximized. The trade secrets held by each collaborator and shared with another collaborator for his/her use during (and possibly after) the collaboration under the agreed terms and conditions are part of the "background IP."

Trade secrets as foreground IP. Trade secrets may also be created as the results of collaboration. In these cases, they are part of the "foreground IP." When the collaboration leads to a new idea (i.e., new information in a broad sense), how to handle that valuable information can become an important question for the collaborating parties. Who has ownership over that new information? Should it be simply published instead of seeking patent protection? Should one seek patent protection, thus also committing to disclosing the information? Or is it better to rely on trade secret protection, which requires a consciously crafted confidentiality regime and conditions of disclosure? Should trade secret information be shared only within the collaborative research group or beyond? If the institutional goals and economic or business interest of the collaborating partners align, it is not so difficult to find a common answer to these questions. However, if their business principles and goals are not pointing in a similar direction, it may be more challenging to find an agreement.

As can be easily imagined, how to best handle trade secrets in collaborative research depends on the agreed objective and nature of the collaborative project. Nevertheless, what can be said with certainty is that **trade secrets are an integral part of collaborative innovation**, and there are several points that organizations should take into account in this setting. See Part VII (Trade secrets and digital objects), in particular, Section 3, for trade secret protection of digital data, metadata, algorithms and code in collaboration.

1. Particularities of trade secret management in collaborative innovation

The general measures of trade secret management also apply to collaborative innovation (see Part IV: Trade secret management). Since the sharing of trade secret information with a party (or parties) outside the organization increases the outbound risk of trade secret misappropriation by a party outside the organization as well as the inbound risk of the organization being contaminated with third parties' trade secrets, Part IV, Sections 3.2 and 5.2 of this Guide highlight some measures to mitigate such risks.

In a collaborative research setting, innovation managers are expected to manage secrecy (trade secret information) and flow of that information throughout the collaborative innovation process. External factors that mitigate the risk of trade secret misappropriation, such as a robust national legal framework for protection of trade secrets, may also support raising the level of confidence and trust between collaborators to the point that they can comfortably share their valuable intangible assets. Below, some general guidance on how to approach the particularities of trade secret management in collaborative innovation are outlined.

1.1 Trust and loyalty in collaboration – legal and cultural differences

Confidence and trust are the keywords for successful trade secret management. Creating trust and loyalty among collaborators will usually reduce the risk of misappropriation. This can be easily said but is difficult to achieve.

Multi-jurisdictional collaboration – legal frameworks

Sharing similar, if not identical, national legal frameworks or legislation among all collaborators would facilitate development of mutual confidence and trust. For example, one of the driving forces for the adoption of the European Union (EU) Directive on the protection of trade secrets is that without effective and comparable legal means for protecting trade secrets across the EU, incentives to engage in cross-border innovative activity within the region are undermined, and thus trade secrets are unable to fulfill their potential as drivers of economic growth and job creation.[1] In reality, however, organizations and individuals involved in international collaboration projects may come from different regions having different legal traditions relating to trade secret protection and enforcement.

While convergence of national legal frameworks on trade secrets has been observed to a certain extent (particularly with respect to the eligibility criteria), laws and practices beyond the trade secret law in the narrow sense, which are relevant to exploitation and enforcement of trade secrets, continue to vary: they include laws regarding employment, privacy and data protection, property and joint ownership, contracts, civil and criminal procedures and technology export controls and taxes. To avoid any misunderstanding and unwarranted expectations, collaborators need to be mindful of the differences in national laws and fill in the gaps with contractual arrangements or a sound choice of law.[2]

Multi-jurisdictional collaboration – cultural differences

Obviously, the underlying legal frameworks represent just one factor that could have an impact on trade secrets in multi-jurisdictional collaboration. Cultural differences among the members of a collaboration team may also affect the behaviors of, and communication among, team members. In the end, a collaboration agreement needs to be executed and trade secret information is shared among individual members. In the international context, training and educational programs on trade secrets can be adapted to a multi-cultural team, also sensitizing the participants about the different approaches to confidence building and information sharing.

1 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, Preamble paragraphs (3) and (4).
2 Issues relating to cross-border litigation is addressed in Part V: Trade secrets in litigation, Section 7.

Differences in organizational culture and business strategy

Even if collaborators come from the same country, their **organizational culture and structure as well as business strategies** may lead to different understandings about, and expectations for, trade secret protection. Typically, in collaborative research between public research centers (including universities) and private companies, protection of trade secrets has different impacts on their respective missions and goals (see Section 3, below). To lower the trade secret management gap, efforts of all parties to align the ultimate objective of the collaborative project is one aspect that should be borne in mind, with due regard to their respective justified interests.

In general, it is more difficult to build a team of individuals coming from multiple organizations. In addition to the organizational culture, confidentiality rules and guidelines applicable to the collaborative research team may be not the same as what is applied to the organization of each team member. Therefore, **clarifying practical rules and expected behaviors** of team members, i.e., to-do and not-to-do, may help team members interact and work together. They do not necessarily need to be formal internal rules and can be provision of guidance to those who are involved in the collaborative project. What may be important is that **all collaborating parties**, both researchers and managers, are involved in setting guidance, which should be clear, consistently applied and in line with the goal of the collaboration. Accordingly, **team building, education and training** for team members play an even more important role in successful collaboration.

1.2 The fuzzy nature of trade secrets in collaborative innovation processes

Terminology

In all collaborations, collaborators should clarify the definition of ambiguous terms such as "open," "secret" and "confidential," which could represent different notions when they are used within their respective organizations. For example, one party may use "confidential" as a broader term, which encompasses concepts such as privacy and security and not only trade secrets.

In addition, the languages of the collaborators may create associations that form their different understanding of the terms. For instance, in Scandinavian languages, the legal term "business secret" is used in the place of the term "trade secrets." Thus, there is a risk that some people may construe the former term more narrowly than the latter, which is more commonly used in other regions. Therefore, the collaborators may need to agree on what is meant by a seemingly common term "trade secret" (or "business secret") in the first place.

Uncertainties in the collaborative innovation process

Product development is a long journey starting from generation of an idea, conceptualization, R&D, product design and manufacturing to marketing and business analysis. The early stage of this innovation process is often referred to as a "fuzzy front end," since the outcome of the process and the appropriation of the innovation are unclear and uncertain. However, **already at this early stage, managing access to information** may be important for keeping the innovation process in a controlled environment.

As a trade secret is a flexible body of knowledge, it can be more difficult for the collaborators to anticipate which trade secret information will need to be shared in future collaborative activities. Therefore, the parties in collaborative activities need to find a balance between clarity of the term and flexibility. Some tips for achieving such balance are provided in Section 2.2.

Moreover, information management at the early stage of collaboration is necessary not only for maintaining the possibility of protecting new ideas (i.e., information) via trade secret protection, but also for **keeping options to seek other forms of IP**, such as patents and industrial designs that depend on secrecy before filing. In this "fuzzy front-end" phase, such confidential and potentially valuable information may or may not satisfy the legal requirements for trade secret protection. At some point, however, confidential information may become trade secrets that

meet legal requirements or may be published or otherwise become common knowledge among researchers in the field. As another possibility, it may continue to be treated as not more than confidential information throughout the innovation process, i.e., while having been kept confidential, its value due to secrecy cannot yet be affirmed.

If this sounds very complicated, the bottom line is that both parties acknowledge the fuzzy and dynamic nature of trade secrets in collaborative innovation and find a practical arrangement not only through their legal teams but also involving business and technology managers.

Tip: Trade secret protection may continue after filing a patent application

To meet the patentability requirement, the claimed invention contained in a patent application must be new: it cannot be part of the information made available to the public. Therefore, information about the invention must be kept confidential before filing a patent application. In other words, such information is a trade secret prior to patent filing.

In most countries, patent applications are not published immediately after patent filing. Therefore, a patent applicant (who is a holder of the information contained in its patent application) may continue to enjoy trade secret protection on that information up to the publication of the patent application.[3]

Consequently, if the trade secret holder continues to make its efforts to keep the information secret before the publication of the patent application, it will retain two options until that time: (i) maintain the patent application, and lose trade secret protection upon publication of the application; or (ii) withdraw the patent application before its publication and maintain trade secret protection.

Both patent protection and trade secret protection have different pros and cons. Since the situation surrounding the technological development and market needs may change quickly, obtaining this flexibility of choice between patent protection and trade secret protection (despite a window of a limited period) can be interesting for trade secret holders.

In cases where trade secrets are shared among the collaborators, it is highly important that both parties strictly observe confidentiality to keep both protection options open as long as possible.

Patent and trade secret protection mechanisms are not always alternatives. Rather, they work in tandem so that organizations stay ahead in competition. More on the complimentary use of patent and trade secret protection mechanisms is found in Part III, Section 3.

1.3 Maintaining oversight of trade secret management

Due to the potential flexible understanding of trade secrets among employees and the fuzzy front end of the innovation, maintaining oversight of trade secret management throughout the innovation process of one organization is already complicated. In a collaboration setting, it usually becomes more challenging, as more organizations, and hence **more IP managers**, are involved.

A practical question for collaborators is whether it makes sense to designate an IP management function for the specific collaboration (such as a steering group or an advisory board) or whether it is sufficient that the IP managers of the different parties find agreement. The greater the differences in terms of the industry sector, nationality or a management approach between the two parties, the more tensions can arise during discussions among the various IP managers. Creating one IP management function in the collaboration team may make sense, particularly

3 In many countries, patent applications are published after 18 months from the filing date (priority date) of the application.

where multiple parties having different management cultures and bringing in a complex set of background IP will embark on long-term projects aiming at ambitious research outputs.

2. Management of trade secrets in different phases of the collaboration

Although most of the general principles and guidance on trade secret management[4] apply throughout the different phases of the collaborative innovation process, particular steps in that process may require more attention.

2.1 Negotiating collaboration

Usually, when two or more parties have expressed their general interest in engaging in collaborative activities, they will assess various positive or negative impacts of such collaboration for their own organization and negotiate an agreement.

During this phase, sensitive business or technological information often needs to be shared among the parties. Therefore, a **non-disclosure agreement (NDA)** is usually signed between the parties. The main features of the NDA are explained in Part IV, Section 2.3. However, there are a few important points to be considered in signing NDAs at this stage of the collaboration.

- **Purpose limitation**: the NDA is strictly for assessing the feasibility and desirability of the collaboration. It focuses on confidentiality and exchange of confidential information. There is no component of licensing clauses and no intent to share anything that goes beyond what is strictly necessary for the negotiation.
- **Identification of the confidential information**: properly identifying what constitutes confidential information is crucial, since sharing of the confidential information takes place in a tentative, uncertain relationship between the parties.
- **Termination protocol**: NDAs should explicitly state that documents and other data carriers as well as materials and prototypes containing the confidentiality information should be **handed back or destroyed**, if the parties decide not to pursue further negotiation. The types of data carriers and destruction methods may be specified, and parties may also require a certification of destruction. In addition, the parties usually guarantee that no further use of the shared confidential information will be made. In some jurisdictions, parties may need to hold shared information for a minimum period of time because of, for example, auditing or legal requirements. Parties may also consider these aspects in negotiating termination protocols.

2.2 Bringing trade secrets into the collaboration

When the negotiation is successful, a formal collaboration agreement usually includes a set of clauses over trade secrets (and/or know-how), including **sharing of the background IP** and **management of the foreground IP**. The NDA concluded during the negotiation phase should be expressly superseded by the collaboration agreement.

While a collaboration agreement usually defines and **lists the background IP of each party**, a clear identification of subject matter is more challenging for trade secrets than for other IP. This is because any leakage of trade secret information could result in loss of protection.

One possible practical technique could be to define a trade secret with a reference to a title or other identifying designation (or an ID-number) and the field of the trade secret concerned in the list of background IP (e.g., *Trade Secret 14, on quality of component manufacturers*). If a collaborator needs to access or use the secret information, a more specific agreement may be concluded. In general, an internal database documenting the trade secrets can be helpful, as it may keep track of access to them by the authorized individuals in the collaborating entities.

4 See Part IV Trade secret management. In particular, Part IV, subsections 3.2 and 5.2 discuss some measures to mitigate high risks of misappropriation and contamination in collaborative activities. Part IV, subsection 2.3 specifically addresses contractual measures to protect confidentiality, including contracts with third parties.

From the perspective of the owners of the background IP, it is also important to specify in the agreement that they will hold the ownership of any **modification of the trade secrets** that form part of the background IP.

To find a balance between clarity of the collaboration agreement and flexibility of future collaborative activities, parties may consider:

- **Clear but flexible NDAs**: NDAs may clearly define confidential information involved in the collaborative activity, and also include a clause that allows for a periodic review and adjustment of the scope of confidential information in accordance with project development.
- **Tiered access to information**: researchers and teams involved in the collaboration may have different level and scope of access to shared information. For example, in a partnership between a university and a pharmaceutical company, early-stage research data may be widely accessible within the university, while access might be restricted to a smaller group when it comes to more commercially viable findings.
- **Defined yet adaptable milestones**: parties may agree on clear milestones for project development. At each milestone, they may review what information has been generated and decide how to treat it.
- **IP strategy meeting**: parties may hold regular IP strategy meetings to maintain ongoing dialogue on managing IP flexibly while maintaining a clear process for decision making.

Sharing background trade secrets held by other collaborating partners means there is more exposure to trade secret information of the other party, increasing the risk of contamination with the trade secrets held by the other party.[5] In accordance with the collaborative agreement, each party should take measures to prevent unlawful use or disclosure of trade secrets held by others.

Even if an impeccably drafted non-disclosure requirement is in place, the risk of unlawful use of background trade secrets by another party cannot be zero. Therefore, from the perspective of trade secret holders, the scope of trade secrets that are included in background IP should be **limited to specific use of specific information for the specific purpose** of the foreseen collaborative activities.

Similarly, from the perspective of another party who is the recipient of the trade secret information, it may not wish to receive any unnecessary disclosure from the trade secret holder, since it will merely extend the obligation of confidentiality to unnecessary information received, and increase the burden of managing it properly to minimize the risk of liability.

2.3 Identifying joint trade secrets in the collaboration

In general, a collaboration agreement also states how **foreground IP should be identified, reported and managed**. Thus, it stipulates how jointly developed IP should be owned, who owns the rights to seek legal protection of the joint IP, who has the rights to use the joint IP, who has commercial exploitation rights, what are the rights after termination of the collaboration and the rights to derivative IP etc. (see also Sections 2.4 and 2.5, below).

To identify jointly owned IP, usually one or more managers, such as a project manager, will be responsible for reporting technical advancement made during the collaboration to an IP manager (or a common IP management group) of the collaborative project. At this stage, the project manager instructs researchers to keep potentially valuable information, ideas etc. confidential. New findings that can be more suitable for patent protection than trade secret protection must be kept confidential at least until filing a patent application. To be potentially protected by trade secrets, the information needs to be handled with a sufficient level of caution to comply with the criteria for trade secret protection.

Based on the report from the program manager(s), the IP manager or management group considers **which type of IP protection mechanisms** may best suit each new technical finding.

5 See Part IV, Section 5.2.

Usually, appropriateness of trade secret protection is reviewed in comparison with other IP, such as patents. Some of the questions asked are: Is maintaining secrecy of the information crucial for long-term commercial success? Will external technological development make the secret information naturally known to other researchers by their self-discovery or become obsolete in a short period?

The answers to these questions have an impact on the expected duration of trade secret protection as well as the required cost and resources for trade secret management. Therefore, decisions will be taken not only from the **legal and technical** perspectives but also from the **business and commercial** perspective. Naturally, if the secrecy of certain information is crucial for long-term success, the collaborators need to take stronger measures to protect it than if the secret information will be revealed anyhow. For the latter cases, collaborators may also consider a revealing strategy to avoid unintended consequences from the natural termination of trade secret protection.

2.4 Handling shared trade secrets during the collaboration

The fact that trade secret information was developed in the collaborative research space does **not necessarily mean that it ought to be held jointly**. Joint ownership of all developed technology may usually seem to be a simple solution. However, since the developed technology often includes pre-existing IP, the owner of such pre-existing IP may inadvertently and indirectly give away its control over the pre-existing IP.

Therefore, depending on the practical needs of collaborating partners in the short, middle and long term, they may agree on an arrangement of a sole trade secret holder with the possibility of lawful use of the information by other collaboration members. Such an arrangement may also take into account the business strategy of each party, such as the main geographical fields of business, the fields of commercial use etc.

In general, such arrangements are negotiated and **stipulated in contracts** agreed by the collaborators. Since some information shared with collaborators can be critically important for the trade secret holder's business, the contracts may contain multiple provisions to reinforce the protection. They include, for example, confidentiality of information, limited use of the information, non-transferability or non-assignability of the information, termination rights after a change in control of a collaborator, and dispute resolution provisions.

Even with these contractual provisions, there is an inherent risk that the persons involved in the collaboration may share the secret beyond what is agreed upon. The collaboration agreement may not be known in detail by all researchers involved. Even if it is known, they may apply the rules flexibly: for example, a researcher may find that the objective of a smoother collaboration justifies not following the rules or even not being in line with the rules.

Therefore, collaborating partners may also agree on additional measures to reassure that the parties comply with the confidentiality obligation. For example, the importance of regular and continuous **educational programs** for all people involved in the collaboration is already highlighted. In addition, parties may agree on periodic audits to review compliance with the agreed terms.

2.5 Trade secrets after the collaboration

The management of jointly owned trade secrets and liability clauses are important not only during the collaboration but also after the end of the collaboration, amicable or otherwise. These clauses related to post-collaboration questions also need to be agreed between the parties and included in the collaboration agreement.

The issues that may be considered are:

- **who will own** which trade secrets once the collaboration ends;
- the **duration** of the confidentiality clauses or NDAs;
- liability in case of trade secret misappropriation or breach;

– reach through clauses, including a party's subsidiaries or eventual licensing, sublicensing or assignment.

A particular concern for the ownership of trade secrets is that if a trade secret becomes public, it loses its entire value. Therefore, collaborators depend on the others' ability to keep a secret even after the collaboration ends. Finding a mutually agreeable solution that protects the confidentiality of trade secrets should be a common interest among all collaborating parties.

The management of trade secret post-collaboration could also require certain care by each party. Thus, when the collaborators discuss how the jointly created information should be protected by different types of IP, they may also consider the potential implication of trade secret protection post-collaboration.

3. Specifics of collaborations including academic partners

Collaborative research involving both public research institutions and industry players has been growing. Around one-quarter of OECD countries each spent over €100 million directly to support the development of collaborations between public research organizations and industry in 2017.[6] The number of PCT international patent applications jointly filed by business and the public sector[7] grew significantly from 2008 to 2022 in many countries: the number increased approximately eight times in China, four times in France and the Republic of Korea and two times in the United States of America.

Traditionally, **universities and public research institutions (PRIs)** have been operating under the principle of openness and information sharing. Many universities claim that openness in knowledge sharing and the absolute freedom to publish are part of their academic mission of education and basic research.[8] Publication of research results was of greatest importance for academic researchers' career development. Therefore, there was not much need for PRIs to consider trade secret protection of their innovation output (apart from national security restrictions).

This position, however, may contrast with the **needs of private sector players** with whom a collaborative research agreement is sought. For industry, trade secrets offer unique protection that cannot be replaced with other protection mechanisms and are part of the valuable intangible assets that strengthen a company's competitive advantage. Regardless of whether the trade secrets are part of foreground IP or background IP, the risk of losing trade secret protection is an important factor for deciding on entering into collaboration with PRIs. Such a fundamental gap of interest and objectives between PRIs and private entities has been narrowed gradually, and parties from both sectors seek synergies and practical solutions in advancing their research.

3.1 Use of trade secrets by universities and PRIs

The increasing research interaction between academia and industry, coupled with a growing emphasis on the commercialization of academic research, has caused a shift in the traditional thinking of universities and PRIs on access to information generated by them, at least to a certain extent. Having said that, the IP policies of universities address protection of trade secrets much less than patent protection. Moreover, the extent to which trade secret protection

6 University-Industry Collaboration, OECD, 2019.
7 Due to the reasons explained in section 2.4 above, collaborating parties may agree that one of them will be an owner of foreground IP. Therefore, the number of patent applications jointly filed by business and public sector does not necessarily show the total number of applications generated by such collaboration. However, since collaborative agreements are confidential, it is very difficult to ascertain the total number.
8 In the United States of America, academic institutions may enjoy the benefits of the fundamental research exclusion (FRE) under export control rules. In essence, the FRE applies if the results of basic or applied research in science and engineering are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial activities.

of their research results is allowed varies significantly among the universities (see section 3.3 for examples of the trade secret policies of some universities[9]).

As outlined in the previous Parts, the decision to protect certain information as a trade secret can be influenced by many factors.[10] Many of the general tips and pitfalls for managing trade secrets, such as identifying trade secrets, evaluating their value and associated risks, maintaining confidentiality, and avoiding unintended use of others' trade secrets, are also applicable to the university settings.[11] However, since university-private sector collaboration often aims to bring together the research expertise of universities and commercialization capacity of the private sector, universities may particularly take into account the expectation of potential industry partners in evaluating the value of the information they possess. It goes without saying that the university's legal and ethical standards and policies provide the framework for identifying and managing trade secrets.

There can be various situations where a university may consider protecting certain research findings as trade secrets. The following paragraphs provide some examples.

Research with commercial potential

More and more countries allow universities and PRIs to file and become owners of patents for inventions created in their institutions. To seek patent protection, the newly created knowledge (i.e., information) must be **kept in secrecy before filing a patent application**. Usually, universities set their own internal mechanisms that require researchers to report any new findings and to keep the information confidential at least during a certain period so that the universities can evaluate its potential IP value and the best way to protect it.

In addition, if certain know-how and newly created knowledge that has not been patented are kept in secrecy, once a potential collaboration opportunity with industry arises, they might become the most relevant information for the collaboration that has been sought. Such **non-patented confidential information as part of the "background IP"** can be a valuable bargaining chip for negotiation with a potential industry partner.

Industry collaboration

There can be different kinds of collaborative relationships between the academic and industry partners. They include, for example, sponsored research where a university's research activity is funded by an industry partner, co-financing research collaboration projects where a university and an industry partner both participate in the research, and commissioned or contract research where a company "purchases" specific research tasks conducted by a university. In general, the stronger the company's control over the research subject, design and planning, the more robust proprietary protection of the research results the company may require. This, however, is not an absolute rule, since each collaboration takes place in a specific environment on a specific research subject.

In **sponsored research** projects, the sponsor will generally require the university and the creators to preserve secrecy of the information. In these cases, universities may have to agree to terms regarding confidentiality. This might mean that certain research conducted in collaboration with a company is kept secret for a set period or until patents are filed. However, due to the freedom to publish principle, some universities will not allow, at least as a general rule, any information generated by its staff members, even under a sponsored research contract, to be kept secret.

Under **co-financing research collaboration agreements**, each party's rights to the joint research outcome, including the handling of jointly created trade secrets, must be agreed

9 See also WIPO Database of Intellectual Property Policies from Universities and Research Institutions, which contains intellectual property policies, manuals and model agreements from universities and research institutions worldwide. https://www.wipo.int/en/web/technology-transfer/database-ip-policies-universities-research-institutions.
10 See Part III: Basics of Trade Secret Protection of this Guide on factors to be considered when deciding whether an innovative output should be protected by patents or trade secrets.
11 See Part IV: Trade Secret Management of this Guide.

between the parties. In one university,[12] its policy states that the joint results must be published in case where the collaboration does not lead to the results that one or both parties had expected. It will ensure that the university researchers involved can still perform research within the area in question after an agreement has been signed with the industry party, and that the researchers have the freedom to collaborate with other companies and organizations. It is possible for the industry party to obtain a license or purchase the project results, depending on who has contributed to what in the creation of the results in question.

In practical terms, each party can have different expectation to the outcome of the joint research. Therefore, in collaborative agreements, success or failure of the collaboration should be determined by objective factors, such as measurable milestones or deliverables, to avoid potential disputes.

In **commissioned or contract research**, the rights to research results usually belong to the industry party who commissioned the research. In general, the industry party prefers to bind university researchers with non-disclosure obligation. However, contract research agreements may be scrutinized by the university to avoid any conflict with the researcher's obligation to the university. The university may also have a policy regarding a restriction to scientific publication of research results under such agreements. However, the general principles or terms of an institutional policy are more often operationalized in the contractual arrangements, such as research agreements, consortium agreements etc.

While collaborative research with industry partners creates an opportunity for university researchers to access a new source of knowledge, it also exposes university researchers to trade secret information held by the industry partner, which university researchers must keep confidential and can use only under the agreed terms and conditions and for a limited purpose. This increases the burden of university researchers to manage the obligation of confidentiality and avoid unlawful use or disclosure of such information. In case of trade secret misappropriation, not only the university researcher but also the university itself may be held liable, depending on applicable national law, university policy and circumstances of the case.

Spinoffs

Universities often support the creation of **spinoff companies** to commercialize research findings. In addition to patents, trade secrets could also be their valuable asset to raise funds and establish their position in the market. Universities may be indirectly involved in protection of these trade secrets as a stakeholder, such as a member of the Board.

As illustrated in the case studies in Subsection 3.4, the interests of the parties involved in spinoffs are not necessarily aligned. Often, a spinoff company itself, a commercial entity that participates in the spinoff with its technology, a financial investor, a university and an individual academic researcher have different interests that form their behaviors and expectations.

Therefore, it is even more important to conclude a **clear and solid contract** that can be relied on by those involved. The key issues relating to trade secrets are similar to any collaborative activities. They include: the scope of the trade secret information assigned or licensed to the spinoff; the scope of the rights of the spinoff to acquire, use or disclose the trade secrets received; and the ownership and right to use trade secrets created in the spinoff's activities.

Competitive research grants

In some highly competitive research areas, preliminary results or methods may be kept confidential to gain a **competitive advantage for obtaining funding** from external sources. Which level of confidentiality over the sponsored research is imposed may depend on, for example, the nature of the sponsors (e.g., government, non-profit foundations, industry etc.). In general, industry sponsors may prefer restricted disclosure of research results. When public sponsors fund public–private collaborative research, they usually design a framework that

12 Research & Innovation, Collaborating with the University of Copenhagen, The University's Overall Principle (2012). University of Copenhagen. https://healthsciences.ku.dk/research-files/KU_s_guide_vedr__samarbejdsaftaler_GB.pdf.

accommodates the need for industry participation on the one hand and the general preference of universities for non-exclusivity and disclosure models on the other.

Material transfer and associated trade secrets

In the field of biotechnology research, researchers may need access to physical proprietary biological materials, such as cell lines, animal models, hybridomas and vectors, to advance their research. A university can be a proprietor of such biological material, which may be, for example, necessary for an industry partner to carry out the collaborative research. In that case, typically, the university and the industry partner who receives a sample of the material conclude a Material Transfer Agreement (MTA), in which the terms and conditions for use of the sample, restrictions on modifications, handling of the material upon expiration of the contract etc. are stipulated.

In some instances, the university also holds **know-how that is associated with the permitted use and storage of the sample** (for example, specific storage conditions to keep the material viable). Such know-how can be the university's trade secret, which needs to be shared with the industry partner to use and store the sample for purposes of the collaborative research. Accordingly, conclusion of a confidentiality agreement in relation to the trade secret between the two parties will be necessary.

3.2 Selected trade secret protection measures in a university setting

If a university decides to protect information as a trade secret, in general, the Technology Transfer Office (TTO) of the university will handle the legal and commercial aspects, such as drafting confidentiality agreements, managing sensitive information and conducting licensing negotiations. When handling and managing trade secret information, TTOs follow the **university's relevant policy** that may outline procedures for disclosing inventions, protecting sensitive information and the sharing of research findings.

General best practices regarding trade secret management can also be adapted to universities.[13] For example, university employees, including researchers and professors, may be required to sign confidentiality agreements, especially when they are involved in research that has commercial potential or when they are working with industry partners. In some universities, the university, and not individual researchers, is bound by the collaboration agreement in a university–industry collaboration setting. Thus, the university has the obligation to comply with confidentiality clauses, and will bear the liability. Some universities require researchers and students who participate in collaborative research with industry partners to sign a confidentiality declaration to fulfill its contractual obligation. Considering the complexity of intellectual property matters in university–-industry collaboration agreements, involvement of TTOs in discussions with protentional research partners from an early stage in the process is advisable.

The particular status of universities requires a few issues that can be highlighted as follows.

Safeguarding publication and future research

From the premise of an academic mission of education and basic research, universities pay particular attention to maintaining the possibility of publishing research results (even if the publication may be delayed) and safeguarding the possibility of and space for future research and commercialization activities on the same research subject.

Some universities include trade secret clauses in their standard collaboration agreements (for example, agreed delay of publication as well as confidentiality terms for background trade secrets and research results). However, their IP policy may allow individual collaboration agreements to deviate from such standard agreements.

13 See Part IV of this Guide.

Organizational management structure

With respect to trade secret management at the institutional level, the organizational and hierarchical management structure of universities is somewhat different from a private business entity. Although the importance of an internal trade secret management structure across the organization applies to both, such differences may be taken into account in designing an organization-wide trade secret management team.

Trade secrets accessed by students and affiliated researchers

A more peculiar issue, however, may be the handling of trade secrets created or accessed by non-employee students and affiliated researchers.

In general, legislative provisions regarding IP ownership in employer–employee relationships and internal guidelines applicable to employees do not apply to undergraduate, postgraduate or PhD students, nor visiting researchers from other universities or other organizations, who are not employees of the university.

However, they may also generate valuable trade secret information through their study or research activities at the university, may be in a position to access trade secret information held by the university, and may be exposed to trade secrets held by external parties by, for example, participating in university–industry collaborations. Consequently, providing clear **guidance on the rights and obligations of non-employee researchers** and setting an appropriate and workable internal management system are important for universities to protect their trade secret assets and to avoid misappropriation of others' trade secrets brought into the university.

Especially for **students** who are not employees of the university, it is necessary to find a balance among educational openness to publish research results, educational merits from participation in university–industry collaboration, and the need to protect sensitive information. In practice, in cases where they will have access to trade secret information, they may be required to sign confidentiality agreements or unilateral declarations. Similarly, a practical arrangement may be found for public defense of theses by students or the availability of theses in the university library. Provided that the university's IP policy allows it, the defense may be done in a closed meeting, or the theses may be embargoed for a specific period.

As university practices vary, clear internal trade secret-related rules applicable to students would be helpful for preventing potential disputes. Students should be well informed about these rules and the possible consequences for them, through educational and training programs.

As to **affiliate researchers**, at least for those whose primary research takes place in the university concerned, applying the same policy and rules as employee researchers may simplify the management of trade secrets. However, in the case of visiting researchers, this may require explicit acceptance of the university's IP policy by the visiting researcher, which may also necessitate an agreement of the sending institution or an inter-institutional agreement in this regard.

Example: IP policy of the City University of London (student version)

The City University of London provides a simplified, user-friendly version of an IP policy publication, which includes protection of trade secrets generated or accessed by students and affiliated staff.

As to affiliate staff (including visiting academics, honorary staff, retired members of staff, and emeritus professors), if their research is primarily focused at the university, they will be automatically deemed to have accepted that they will be treated as if they were employees of the university (solely for the purposes of the IP policy) as a condition of being granted access to the university's premises or facilities. Accordingly, they will be required to assign any IP that they may generate during their engagement in research at the university. The university may

require affiliate staff (and/or their home institution as appropriate) to sign an agreement to give effect to the IP ownership question.

The publication also reminds each individual to contact the responsible unit as soon as possible, if they believe that they have created an invention or generated other IP.

The policy also cautions the university staff and students to be alert to IP owned by third parties (e.g. other universities, companies or funding bodies). To respect third-party IP and not to infringe third-party IP rights, university staff and students intending to use any materials or IP provided or owned by third parties must ensure that they and the university are authorized to do so. Although research or teaching use may come within exceptions to the relevant IP law, this should not be assumed, as the law in this area is complex.

Regarding the ownership of IP generated by undergraduate and postgraduate students during their studies or research, the students will generally be the first owner of that IP. However, they will be required to assign their IP to the university, under certain circumstances. These circumstances are: (i) the IP is generated under contract terms with a third party that require the IP to be owned by the university or a third party (for example, under a funded studentship); and/or (ii) the IP is generated together with the university's employees, or the IP builds on other IP previously generated by university employees.

All students will be automatically deemed to have accepted this requirement to assign their IP to the university in these circumstances as a condition of being accepted for admission to their degree program. Where a student is required to assign their IP to the university, the university may require the student to sign an agreement to record the ownership issue formally. In return, the student will be treated in the same way as an employee of the university solely for revenue sharing purposes under its IP policy.

As to affiliate staff (including visiting academics, honorary staff, retired members of staff, and emeritus professors), if their research is primarily focused at the university, they will be automatically deemed to have accepted that they will be treated as if they were employees of the university (solely for the purposes of the IP policy) as a condition of being granted access to the university's premises or facilities. Accordingly, they will be required to assign any IP that they may generate during their engagement in research at the university. The university may require affiliate staff (and/or their home institution as appropriate) to sign an agreement to give effect to the IP ownership question.

The publication also reminds each individual to contact the responsible unit as soon as possible, if they believe that they have created an invention or generated other IP.

The policy also cautions the university staff and students to be alert to IP owned by third parties (e.g. other universities, companies or funding bodies). To respect third-party IP and not to infringe third-party IP rights, university staff and students intending to use any materials or IP provided or owned by third parties must ensure that they and the university are authorized to do so. Although research or teaching use may come within exceptions to the relevant IP law, this should not be assumed, as the law in this area is complex.

Source: City University of London, Intellectual Property Policy (Student version), available at: https://www.city.ac.uk/__data/assets/pdf_file/0005/586607/IP-Policy-update-May-2021_student-version.pdf. Although this publication does not contain detailed guidance on the handling of trade secrets in the university research, it is included in the Guide as an example of a simplified version of the general IP Policy, specifically adapted to students.

3.3 Examples of trade secret policies and guidelines of universities

The more universities collaborate with diverse external partners, the more such partners seek clarity of universities' policies regarding trade secrets. As there is no one policy that fits all, universities are applying different kinds of trade secret policies and guidelines.

While the breadth and depth of the policies and guidelines relating to trade secrets vary significantly, they may touch upon: (i) the university's general principles regarding protection

of research results via trade secrets; and (ii) circumstances under which trade secret protection may be acceptable in collaborative research with industries. Specifically, they may cover various issues, such as:

- who may sign confidentiality agreements
- under which conditions trade secret protection may be allowed or preferred
- any restrictions on technology areas that may seek trade secret protection
- whether and under what conditions any additional delay in publication of research outcomes can be permitted
- how students and affiliated staff may be involved in academic–industry collaborative research
- mechanisms for monitoring compliance with the university's trade secret policy and guidelines as well as addressing trade secret breach.

Some examples of the policies and guidelines are illustrated below.

Stanford University[14]

The Industrial Contracts Office (ICO) negotiates research agreements with industry on behalf of Stanford for our faculty researchers. Its goal is to bring funding and materials into university labs to support university/industry research relationships.

In principle, Stanford University maintains a core policy of no secrecy in research. However, the Research Policy sets limited circumstances where a research program shall be regarded as requiring secrecy, which include industry sponsored research, national security controls and protection of privacy.

In the case of research under industry Sponsored Research Agreements (SRAs), while respecting the needs of industry partners, the university prefers that companies do not disclose trade secret information to Stanford employees and other persons associated with it. This also comes from the fact that the university cannot fully monitor who has access to specific information.

However, if the sharing of trade secrets is necessary for conducting a particular project with the industry, the individual researchers may personally enter a non-disclosure agreement. Generally, Stanford is not a party to these agreements. In other words, a Stanford researcher may personally sign a confidentiality agreement on his or her own behalf under certain conditions. Specifically, a researcher must follow the university policy and comply with laws, and the confidentiality terms must be consistent with researcher interests. For example, confidentiality agreements should not create obligations that restrict or redirect research. In addition, a researcher may not sign an agreement that could affect the IP rights of Stanford or its other researchers. Stanford may also be able to accept certain confidentiality terms as part of an SRA, provided they are consistent with researcher interests and in compliance with the university policy.

In a program of sponsored research, a contractual agreement between Stanford and the sponsor may include provision for a delay in the publication of research results. The types of delays accepted are, in general:

- for a short delay for patenting purposes or for sponsor review of and comment on manuscripts (not to exceed 90 days)
- for a longer delay in the case of multi-site clinical research (not to exceed 24 months from the completion of research at all sites).

When it is in the best interests of the research, the University may approve contractual arrangements that could lead to longer publication delays.

14 Researcher's Guide to Working with Industry, https://ico.stanford.edu/sites/g/files/sbiybj16441/files/media/file/researchersguidetoworkingwithindustry_0.pdf; Research Policy Handbook, 1.4 (Openness in Research), https://doresearch.stanford.edu/policies/research-policy-handbook/conduct-research/openness-research.

With respect to students and trainees, a faculty member must not engage a student or trainee in a project governed by an extended publication delay agreement or contractual arrangement that could present a barrier to the timely submission of the student's thesis or dissertation or to the publication of a trainee's work.

The ICO may review the confidentiality agreements vis-à-vis the university policy.

University of Copenhagen[15]

The University's Tech Transfer Office at Research & Innovation is responsible for negotiating various collaboration agreements between the university and external parties. In all such agreements, it is a prerequisite that researchers of the university are able to publish their research results and use them for research purposes.

Publication of research results, produced in collaboration with the University of Copenhagen, can usually be delayed by a maximum of three months (one month where the external party can comment on the material that is to be published, and two months where the company can patent its own results). This period may be divided differently.

However, recognizing the position of private companies that tend to protect confidential information to maintain a competitive position, non-disclosure of an external party's confidential knowledge can be agreed up to a period of three years from the end of a collaborative project. This period may be extended, if specific circumstances justify.

Non-disclosure agreements or confidentiality agreements are used when the external party and the university's researcher(s) exchange confidential knowledge related to a specific research project. Together with the external party, the Tech Transfer Office will assist in defining a narrow agreement that suits both the university researcher and the external party.

Northeastern University[16]

In principle, according to its Policy on Openness in Research, Northeastern University does not undertake research with restrictions on openness or academic freedom on its campus. Examples of unacceptable restrictions include required external approval of research results before publication or exclusion of members of the university community, including students, from participation in educational and research activities.

While most research can be conducted in accordance with the ideals of freedom of inquiry and open exchange of knowledge, the policy recognizes that, in a few compelling instances, the best interests of society will weigh against broad participation in research and open exchange of information. In these cases, exceptions to such principle may be granted. Exceptions will be rare and will require that the research is critically important to the university's mission and serves a demonstrable greater good.

As regards computer software, firmware and databases owned or controlled by the university ("Computerware"), the university's Policy on Trade Secrets states that since copyright or patent protection alone may be inadequate for their protection, they shall be maintained as trade secrets until released by the university. The university may identify other materials to be treated as trade secrets. In principle, faculty, staff and students who create trade secret information shall assign their title and interest in such information to the university.

The Policy on Trade Secrets also clarifies that computerware and other trade secret information may be provided to the university from outside sources under conditions restricting their use or disclosure. In these cases, individuals authorized to access such materials shall treat them as required by the terms agreed between the outside source and the university.

15 Research & Innovation: Collaborating with the University of Copenhagen, The University's Overall Principle, https://healthsciences.ku.dk/research-files/KU_s_guide_vedr__samarbejdsaftaler_GB.pdf.
16 Policy on Openness in Research, Policy Number 503, https://policies.northeastern.edu/policy503/; Policy on Trade Secrets, Policy Number 208, Section III, https://policies.northeastern.edu/policy208/.

Kyushu University[17]

Kyushu University considers that universities are expected to respond to the needs of society by also pursuing collaborative innovation with industry. Therefore, proper management of confidential information that is shared with, or generated with, industry partners is important for the university to develop trusted relationships with them. In that light, the university issued its Trade Secret Management Guidelines in 2012.

In essence, the guidelines cover trade secret information independently created by university researchers or jointly created with industry partners as well as trade secret information of companies that is brought into the university through, for example, collaborative research projects or internship activities of university students.

The guidelines state that, bearing in mind that research results of the university must be made public, the trade secret information may be kept confidential only during the period specified in the non-disclosure agreement or joint research agreement, or as long as required by the university.

When concluding a non-disclosure agreement or joint research agreement, the agreement should include detailed clauses regarding handling of trade secrets and appointment of a responsible trade secret manager. The highest level of care should be given to students who participate in joint research so that they will not be disadvantaged by the confidentiality obligations, such as being restricted from presentations at academic conferences.

If joint research is conducted with multiple companies, efforts should be made to avoid contamination of information transferred from/to each company by, for example, separating the locations of joint research activities. In addition, with respect to exchange of undisclosed research information with overseas institutions, the security or export control should be conducted, as appropriate, in accordance with the procedures stipulated by the university.

In the event where the university has the right to a patent, the relevant information shall be kept confidential so as not to lose the novelty of the invention. In addition, trade secrets received from companies that are legitimate holders of trade secrets should be properly managed in accordance with the confidentiality clauses in the non-disclosure agreement or joint research agreement, and in compliance with the agreed management procedures and purpose of use.

3.4 Illustrative cases of university–industry collaboration

To highlight how trade secrets could become relevant in university–industry collaborative research in a complex manner, two hypothetical illustrative cases are presented in this Section.

Case A: A chaotic university–industry collaboration: developing animal feed with patents and trade secrets

A Research Team of University X, headed by a prominent Professor, developed a new type of poultry feed, mainly for chicken. The important new feature of this feed related to nutrients, sustainability and handling properties of the feed's composition.

Patent applications PA 1, PA 2 and PA 3 in the field of poultry farming were filed through the university's Technology Transfer Office (TTO). PA 1 and PA 2 were filed on the same day, around a year ago, and PA 3 was filed one month ago. They have not been published yet.

A collaboration between the University and the Feed Producer led to the creation of a Spinoff company. Both the TTO and the Feed Producer were shareholders of the Spinoff, together with an Incubator. Further, the Professor and key staff members of the Research Team had shares and future options to buy more shares, if they became employees of the Spinoff. To start with, the Professor agreed to a 20 percent position with the Spinoff and continued being a professor at the University.

17 Kyushu University Trade Secret Management Guidelines (*Kyushu Daigaku Eigyouhimitsu Kanri Shishinn*).

The Spinoff got an exclusive license from the University for the technology described in the patent applications PA 1, PA 2 and PA 3 and resulting patents. Further, the Spinoff paid the University's Research Team for work on the development of the technology.

As to the technology disclosed in PA 1 to PA 3, the Research Team wanted to publish the principles disclosed in PA 1 and PA 2 in a scientific journal and present the findings of PA 3 at a conference. However, a clause in the exclusive license from the University to the Spinoff allowed the content of the patent applications to be kept as a trade secret for 18 months from the respective filing date, which reflected the interest of the Feed Producer in investing in the Spinoff. The tension between the Research Team who wanted to publish the research findings and the University who signed the exclusive license led to conclusion of a framework agreement between the Spinoff and the University. The framework agreement regulates, among other matters, that University staff who participate in the activities of the Spinoff shall be bound by the confidentiality rules of the Spinoff, i.e., they shall maintain the confidentiality of the information and data generated through the activities of the Spinoff, unless instructed otherwise. In parallel, the Spinoff started developing production methods of the new feed.

Meanwhile, the Professor had made some progress with the commissioned work for the Spinoff. The Professor had found an association between the dosage of one of the nutrients disclosed in PA1 and PA 2 (N1) and the survival rate of chickens. Further, the Professor's understanding of the biological role of N1 would apply to all vertebrates, including fish and mammals. The Professor had not discussed this with the other members of the Research Team, but with the CEO of the Spinoff and its Board members, including those from the Feed Producer and the Incubator. There were no board members from the University. The Professor found the findings to be of great importance for animal welfare and wanted to publish the findings immediately.

However, the Spinoff wanted to keep the findings as a trade secret and not even file a patent application. The Spinoff pointed to a clause on confidentiality in the framework agreement between the Spinoff and the University as well as the Professor's employment agreement with the Spinoff, which obliged the Professor to keep any information obtained from his research activities with the Spinoff confidential. The University initially stood on the side of the Professor, noting that the framework agreement referred to the general clause in the University's regulations, which include the norms of publication and importance of using knowledge for advancing research and supporting education. However, seeing the significant importance of this finding for the future of the Spinoff, the University agreed that the Professor's new findings would be kept as trade secrets of the Spinoff.

However, the Spinoff wanted to keep the findings as a trade secret and not even file a patent application. The Spinoff pointed to a clause on confidentiality in the framework agreement between the Spinoff and the University as well as the Professor's employment agreement with the Spinoff, which obliged the Professor to keep any information obtained from his research activities with the Spinoff confidential. The University initially stood on the side of the Professor, noting that the framework agreement referred to the general clause in the University's regulations, which include the norms of publication and importance of using knowledge for advancing research and supporting education. However, seeing the significant importance of this finding for the future of the Spinoff, the University agreed that the Professor's new findings would be kept as trade secrets of the Spinoff.

All those discussions with the CEO of the Spinoff, its Board members and University representatives made the Professor completely exhausted. To lift his spirit, the Professor met his Friend who was also an old colleague. The Friend suggested, in confidence, that they should investigate N1 and how it affected growth in fish. Rejecting the Friend's proposal seemed strange, as it would advance science, the Professor thought. There would be many benefits for humankind, and it would create more commercialization options. The Professor felt that keeping his research findings confidential was a huge personal burden. Lying and saying "it would not work" was ethically not an option. The Professor initially gave an unclear response, hoping the problem would go away. However, his Friend returned with a draft application for funding a joint research project. The Professor agreed to work with his Friend on the application.

The Professor had the following considerations in mind on the confidentiality and keeping N1 as a trade secret:

- I have signed non-disclosure agreements in the field of chicken feed. I cannot tell him that I know a group of nutrients, including N1, works well for chicken, at least for now. However, the discussion with the Friend is about fish feed. So, for the time being, I will only tell him that I work for the Spinoff on poultry feed. When PA 1 and PA 2 will be published in six months or so, it will become public that the group of nutrients, including N1, influences chicken growth. Then, I can suggest that my Friend should further investigate this group of nutrients. If we find that N1 also works with fish, we can assume that it also works with mammals. Nothing of this concerns chickens.
- We can then follow the policy of the University and file a patent application. We should also be able to publish the finding immediately after patent filing, in accordance with the University's policy.
- Even if the new finding about fish or mammal feed becomes public information, it is not a problem for the Spinoff, because it does not affect the patentability of PA 1, PA 2 and PA 3.
- Even though I am employed and a shareholder in the Spinoff, I am first a Professor at the University. My ethical conviction is more important than the Spinoff's business.

Comments on Case A

Case A demonstrates gradual development of technology that leads to the expansion of stakeholders with various conflicting interests coming onto the scene. We can observe that, slowly, protection of the trade secret is in danger. The case illustrates the complexity of handling secrecy in academia/university and industry collaboration, and the different norms and objectives of different parties involved.

From this case, various positions and perspectives of the main stakeholders can be highlighted as follows:

- **University**: it cares about its mission of advancing research and supporting education, but is also keen on demonstrating its research outcomes (in this Case, through success of the Spinnoff).
- **Spinoff**: it is primarily interested in bringing its first product (poultry feed) to the market. However, it should also have a strategy for subsequent products. The Professor's new finding suggests potential R&D areas and new business opportunities. It makes a business sense to investigate more on that finding under secrecy so that it can be ahead of other researchers and businesses.
- **Feed Producer**: the company is concerned about return on their investment and looks for successful sale of a new poultry feed product through its distribution channel. Like the Spinoff, it may also be interested in even bigger return from the sale of subsequent feed products for mammals and fish.
- **Professor**: he values academic freedom. He is also eager to share his knowledge and tell the world about his new discoveries. In this Case, he believes that his new finding should be shared with others because it is of great importance for animal welfare. His value is more important than Spinoff's business (although the Spinoff and the Feed Producer would eventually commercialize and distribute new useful products based on his research findings).

Not unusually for academics, the Professor has several roles: a Professor at the University and an employee in a Spinoff. The Professor also has a personal relationship with another prominent researcher, who is his friend. The friendship creates another incentive to bend the formal rules. The Board of the Spinoff did not see the potentially conflicting interest of the Professor that could emerge from these different roles. Perhaps a lack of involvement of the University in the Board of the Spinoff also contributed to the oversight.

In addition, the ambiguity of the clauses in the initial contract for the creation of the Spinoff as well as the framework agreement between the University and Spinoff appears to have led the parties to interpret these clauses as they prefer. They could have drafted the NDAs and collaboration agreements with due consideration to possible future development, such as

application of trade secret information in other domains or inclusion of clauses that establish a framework for periodic review and adjustment.

If the University's TTO and the Spinoff had had a broad picture of all parties involved, with clarity on each person's rights and obligations as well as the legal consequences of breach of their obligations under the applicable law, the University's regulations, and contracts, they could have better mitigated the risk of losing a potentially important intangible asset.

Beyond the contractual agreement, the Professor was clearly not aware of the critical importance of trade secrets for the Spinoff and for the commercialization of his important scientific findings. If he and his Research Team have been well educated on the importance of trade secrets and confidentiality obligations, they might think more carefully when there is a temptation to disclose the trade secret information to third parties.

Moreover, there is no guarantee that, after their publication, the patent applications PA 1, PA 2 and PA 3 will be granted as expected. Therefore, if the Spinoff will not be able to maintain the new findings of the Professor as trade secrets, it will be without control of its core business asset and will lose its competitive advantage.

Case B: Proprietary Software in a Collaboration –An Industry Collaboration Falling Apart

Company A is good at developing technology. Company B has a great sales and marketing organization. They decide to collaborate in the IT communication field, bringing together their respective strengths. B asks A to develop a hardware and software IT communication product (P). They agree that A will own the intellectual property derived from the new technological development.

They sign a contract with few details on IP. B gets an exclusive license from A to offer the sale of, and sell, the product covered by A's intellectual property. The product P is sold under both A's and B's trademarks. As agreed, initially, B sells the product exclusively, co-branding it A + B.

The communication protocol used in P is based on an industry standard (S). In the standardized protocol, a subset of messages can be explicitly defined for a product. A has spent much time developing these messages and considers them its trade secret. However, the messages are documented in manuals and documentation for system integrators. They are not marked as confidential and have been distributed without specific non-disclosure agreements. Several messages have been shown in detail as examples in a scientific paper, explaining how the industry standard can be adapted to specific products. The subset of messages can be reverse-engineered, as the communication is not encrypted. As agreed in the signed contract, A provided all information about product P to B, and concluded a non-disclosure agreement with B on the information relating to the product-specific messages.

After some years, A develops a new version (P1) that is also based on the industry standard (S) and the product-specific messages. P1 is sold under the sole brand A. Upon agreement with A, B also sells this new version of the same product line, even if it is no longer an exclusive seller in the market. The original contract is not formally renegotiated.

Gradually, A starts selling other products in competition with the products of B. B's sales manager responsible for marketing A's product is offered a position with A and leaves B.

The sales manager has knowledge of the market that B considers to be its trade secrets. B has not used non-compete clauses in the employment contract with the sales manager. However, before the sales manager leaves B, they agree on which knowledge of the sales manager is a trade secret that she cannot use at her new position in A. They also agree to review the trade secret status of the knowledge under question every six months.

After one year, B confirms that the marketing knowledge concerned has become known among IT communication companies, and the secrecy around that knowledge has ended.

Facing competition, B's sales of P and P1 decline. Eventually, B decides to develop and sell a new product that can compete with the best-selling products of A, i.e., P and P1. Since B does not have sufficient technical capacity, it contacts a trusted developer D, and gives them access to all information they have on product P, including the documentation on the product-specific messages. The new product is launched by B, under the co-branding B+D.

A sues B, seeking preliminary injunction. A claims that B has misappropriated their trade secrets. Further, A claims that the non-disclosure agreement in the original contract is still valid. The court however sides with B, as B can show that A did not take appropriate measures to keep the product-specific messages secret, and that the information is publicly available or can easily be reverse-engineered. Consequently, the information about the product-specific messages was no longer trade secret information when B disclosed that information to developer D without any consent of A.

Comments on Case B

Firstly, if A considers that the information about the product-specific messages is a valuable trade secret, it should have managed that information properly. Trade secrets must be managed from their conception. This need for management contrasts with copyright. In software development, copyright management in the form of knowing who wrote what parts is performed automatically by the systems, and most firms use version control of the code. However, if parts of the code are to be trade secrets, there is an immediate need to manage those parts.

When A provided all information about product P to B, A concluded a non-disclosure agreement with B as far as information about the product-specific messages is concerned. However, subsequently, A did not take the necessary measures to keep the information secret. That led to the valuable information no longer being protectable by the trade secret system. Disclosing the information in manuals, communicating the information without non-disclosure agreements, not using encryption, or using the information in the scientific paper could have been simply avoided.

Since the market environment and business needs of companies change, the collaborative and competitive relationship between two companies develop over time. Thus, the original collaboration agreement could have been renegotiated when a new collaboration/competition relationship between A and B emerged, for example, the development and sales of a new version of the product P1 by A. That could have helped both A and B to review their IP assets, including trade secrets, and re-align the collaboration with their respective new IP and business strategies.

B handled their commercial trade secrets well in setting up an agreement with the sales manager upon her departure from B. Once the employment contract is terminated, to what extent an employer can limit employees to use their knowledge that has been acquired during the employment is a sensitive issue, which also depends on national legislation. In this case, they agreed on which information to be kept secret post-employment and on a mechanism for regular review mechanism. Having such a mutual understanding upon departure of the employee can help avoid future disputes and also avoid the unnecessary burdens on both parties to maintain the secrecy of information that is no longer trade secrets.

More fundamentally, A should have thought twice whether trade secret protection is the best option to maximize the business return from its product-specific messages. In general, a communication protocol would be difficult to keep secret and will become known sooner or later. For example, A could have taken the credit for making the subset of messages open source, instead of assuming trade secret protection.

Part VII: Trade secrets and digital objects

Topics covered in this Part:

- **Categories of digital objects, including digital data**
- **Eligibility of trade secret protection for digital objects**
- **Management of digital trade secrets**
- **Challenges and risks of digital trade secrets, cyber-attacks, audits**
- **Trade secrets vs. other IP rights for digital objects**

With the rapid advancement of digital technologies, businesses face unique challenges in protecting their valuable proprietary knowledge and information. While the "traditional" patent-centric intellectual property protection strategies may still be valid in this technology sector, trade secret protection has emerged as one of the crucial protection regimes for digital technologies.

Since trade secrets potentially cover a wide range of digital data and information, for the purpose of this Part, the term "**digital objects**" is used. It generally refers to **data or information that is stored and transmitted in electronic or digital formats**. Consequently, trade secret protection of digital objects may encompass two distinct areas:

- **digital data** (in a text, audio or image format), **algorithms** or **programming code** as such is valuable trade secret information, and
- trade secret information in any technical field, stored in a **digital format** (such as information about a method of manufacturing substance X stored in a digital file).

In Part VII, we primarily focus on the first category of the "digital objects." However, the IT security measures addressed in Sections 4 and 6 in this Part may apply to any trade secret information in a digital format (see also Part IV: Trade secret management in general and Section 2.3, in particular).

1. Emergence of digital objects and potential for trade secret protection

Digital objects play a pivotal role in today's business environment. With the advent of cloud storage and computing, electronic communications, advanced data analytics, and large language models like GPT-4, organizations rely heavily on digital platforms. The nature of digital objects presents both advantages and challenges for trade secret protection.

On the one hand, digital formats allow for efficient storage, replication, computation and transmission of information. On the other hand, these very characteristics also increase the risks of unauthorized disclosure, theft or exploitation, based on the ease with which digital data can be copied, shared and disseminated.

To be eligible for trade secret protection, digital objects need to meet the basic requirements for trade secret protection, i.e., they need to be:

- commercially valuable because they are secret,
- known only to a limited group of persons, and
- subject to reasonable steps taken by the rightful holder of the information to keep it secret, including the use of confidentiality agreements for business partners and employees.

To determine the eligibility of digital objects for trade secret protection, it is necessary to analyze the subject matter of the "digital object" and identify whether its secrecy makes that subject matter commercially valuable – before addressing specific access-control and confidentiality schemes.

2. Subcategories of digital objects and eligibility for trade secret protection

Digital objects comprise various elements such as algorithms, code (source and object), text, images, audio and video. When considering trade secret protection, there are very important nuances between various subcategories of digital objects and their commercial value.

Algorithms

Algorithms are the backbone of digital data processing. They are sets of rules or instructions that define a sequence of steps to solve a specific problem or accomplish a particular task. Algorithms play a crucial role in transforming raw data into meaningful information through data analysis, machine learning and artificial intelligence applications. They provide the logic and computational framework that allows digital data to be processed, analyzed and interpreted to derive valuable insights. As such, algorithms are at the very heart of digital economies, enabling data-driven decision-making, predictive modeling and automation.

Code

Code, also known as computer code or programming code, is the language used to write software programs and to execute algorithms. It consists of a series of instructions and commands that direct computers to perform specific tasks or operations. Code serves as the bridge between human intent (source) and machine execution (object), enabling the translation of algorithms into executable programs. Through code, raw or pre-processed data is transformed, changed and presented in ways that deliver desired functionalities and user experiences. Code is the fundamental building block of software applications, systems and platforms that harness and use digital data.

Raw data and processed data

Raw data can be seen as the most fundamental form of data provided as an initial, unprocessed output that is obtained directly from data sources, e.g., a stream of numeric values or readings from a sensor captured over time, or unstructured text documents or messages. Raw data is data in its most granular and detailed form, consisting of individual data points or records, and usually characterized by its lack of structure or organization, and it may require preprocessing, cleaning and formatting before it can be effectively analyzed or used for decision-making purposes. It serves as the foundation for subsequent data processing steps, such as data transformation, aggregation, analysis and visualization.

Raw data, in and of itself, is generally not considered for trade secret protection as it typically is the analysis, insights or processes derived from that data that hold the potential for trade secret protection. However, it is important to note that there can be exceptions and nuances to this general rule. In some cases, raw data may have commercial value if it is unique, difficult to obtain, is associated with a particular object, location, party or individual, and its collection methods are proprietary.

In contrast to raw data, processed data is data that already has undergone some form of algorithmic or analytical processing to extract meaningful insights or transform it into a more structured and usable format. Processed data is typically more refined, structured and tailored to specific objectives or analysis requirements – and as such of higher commercial value than raw data.

Metadata

Metadata refers to descriptive information that provides context, structure and additional insights about (other) digital data, be it raw data or processed data. It includes attributes such as the creation date, author, file format, size, location and relationships with other data elements. Metadata serves as a form of data about data, facilitating organization, searchability and interoperability of digital information. It helps users understand the content, source and characteristics of data, making it easier to locate, retrieve and analyze specific information. In the context of digital data, metadata plays a vital role in data management, data integration and data governance processes.

Together, algorithms, code and metadata form the foundation for the aggregation, processing and interpretation of (raw and pre-processed) digital data. As the digital landscape continues to evolve, these components will remain essential in utilizing the power of digital data for innovation, problem-solving, automation and decision-making in various domains and industries.

Digital objects in a traffic information app

To facilitate understanding of the subcategories of digital objects, we could consider a comprehensive traffic information app as an illustrative example of an end product that encompasses various digital objects.

A traffic information app utilizes a combination of algorithms, code, text, images, audio and video to provide real-time traffic updates and navigation assistance to its users.

- **Algorithms**: the exemplary app employs complex algorithms to analyze data from various sources, such as GPS signals, traffic cameras and user-generated reports, to determine traffic congestion, optimal routes and estimated travel times.
- **Code (source and object)**: the app's source code is the underlying programming instructions that dictate how it functions. Compiled into object code, this enables the app to execute seamlessly on users' devices, facilitating smooth interaction and data processing.
- **Text**: through a user-friendly interface, the app displays textual information, such as current traffic conditions, accident reports, road closures and suggested alternative routes. Users can easily read and understand the textual updates and directions provided by the app.
- **Images**: the app integrates images from traffic cameras strategically positioned across roadways, offering users visual insights into real-time traffic conditions. Users can view snapshots or streaming video feeds of congested areas, accidents or construction sites to make informed decisions.
- **Audio**: to enhance user experience and safety, the app provides auditory cues and directions. It may use audio notifications to update users on upcoming turns, lane changes or traffic incidents, allowing drivers to focus on the road while receiving critical information.
- **Video**: incorporating video clips or animations, the app can present dynamic visual representations of traffic flow and road situations. For instance, it could display animated maps illustrating traffic patterns or use video overlays to highlight specific incidents and detours.

By encompassing these elements within its digital framework, the exemplary app epitomizes the term "digital objects," showcasing the diversity and integration of algorithms, code, text, images, audio and video to deliver a comprehensive and interactive traffic information solution to users.

3. “Confidentiality” of digital data, metadata, algorithms and code

To meet a very fundamental prerequisite for trade secret protection, digital objects need to be confidential. This is, in fact, the biggest challenge in practice as organizations share, handle and

process various digital objects on a daily basis. Ensuring confidentiality is essential to safeguard sensitive data, algorithms and code from unauthorized exposure or exploitation.

3.1 Raw and processed digital data and metadata

Collection of data

IoT (internet of things), cell phones, payment processing terminals and other electronic communication devices gather hundreds of millions of data points a day. The mere fact of data collection itself is not necessarily a trade secret, but **"how" and "what" is collected** may lend itself to some type of protection.

For example, an industrial IoT device may use proprietary sensors or other means to collect operating parameters that were not previously obtainable, thus creating a unique data set. If that dataset is encrypted at the time of collection, then the owner could argue that such data is a trade secret because "encryption" would be a reasonable step to maintain secrecy. Similarly, the mere fact that a credit card processor obtains a consumer's spending behavior at point of sale is not trade secret, but what it collects, and in what format, may be trade secret – especially if it is associated with metadata that is not easily obtainable by the consumer or merchant.

Data collected on behalf of a third party

What about data that is collected on behalf of a third party or data that is not "owned" by the collector or processor? These scenarios raise important questions around asserting trade secret protection. As mentioned above, trade secrets are an intangible asset, thus only the data owner (or exclusive user in certain jurisdictions) can assert the intellectual property right.

Data collected on behalf of a third party usually arises in a consulting or vendor style relationship, where the collector and data generator are in contractual privity. The contract terms typically govern who owns what type of data (e.g., raw or processed) and how the parties should treat such data. Asserting trade secret protection on such data will require a contractual review to determine who is the true owner and associated confidentiality/use restrictions. For example, an industrial IoT company that installs and manages IoT sensors will most likely have a service contract with the data owner that governs, among other things, what type of data are collected, how the data are managed, how the data are processed, and the respective rights to use such data. In this situation, both the IoT company and data owner can likely claim trade secret protection on certain aspects of the data.

Collected data without contractual relationship

Conversely, data collected and processed by a third party without contractual privity may be eligible for trade secret protection: but who can assert such protection is a murky issue. These situations most often arise in the consumer context where a payment processor, point-of-sale vendor or other parties involved in the processing of consumer payments handles consumer data. If a credit card is used, the consumer may be in contractual privity with the card issuing bank that dictates the type of data collected and use rights, but is most likely not in privity with the merchant, point-of-sale vendor or processor (e.g., VISA).

Here, each party may "claim" trade secret protection on certain aspects of the data, but who else within the payment chain also has access to the data, and is there contractual privity that governs confidentiality and use? Without clearly defining these limitations (and establishing clear ownership or exclusive use rights), such data may not fall within the definition of trade secrets. The next section will explore these use rights in more detail.

Exchanging and sharing of data

With the advent of social media, e-commerce, industrial analytics and digital economies, data sharing (e.g., via application programming interfaces (APIs)) and commercial data re-sale have become increasingly vital for commercial applications. The importance of data sharing lies in its ability to foster collaboration and accelerate progress. In an era characterized by vast amounts of data being generated across diverse disciplines, sharing data allows researchers

to access a broader pool of information, facilitating cross-disciplinary insights and discoveries. Today, APIs play a crucial role in enabling seamless integration and interoperability between different systems and platforms by providing standardized interfaces for data access and communication.

Furthermore, the rise of commercial data re-sellers and data-sharing agreements has opened up new opportunities for everyone to access valuable datasets that were previously inaccessible or too time-consuming to collect. These re-sellers curate and aggregate data from multiple sources, applying advanced analytics and quality control measures, making it readily available for scientific endeavors. While challenges related to data privacy, ethics and data quality persist, the increasing **importance of digital data sharing, APIs and commercial data re-sellers** signifies a paradigm shift towards collaborative and data-driven research, ultimately enhancing scientific knowledge and innovation across domains.

Shared data with limited access

This new collaborative dimension of data can make it difficult to determine whether specific digital data is a trade secret – who has access to it and which reasonable steps have been taken by the rightful holder of the information to keep it secret – and if so, how to manage and exploit the trade secret.

In practice, confidentiality for shared data (raw, processed and metadata) is often established, where applicable,[1] by applying the **concept of "shared data with limited access"**. The shared data may include information that is not necessarily confidential or exclusive but requires controlled access for privacy or security reasons. **Physical access** to this data is typically restricted through user authentication, access-control lists, role-based access control, encryption and other security measures.

There is most often a **contractual access** control as well. The purpose of limited access is to ensure that only authorized individuals can view or use the shared data, while still enabling collaboration and information exchange within a defined and trusted network of users. When trying to assert trade secret status for shared data, the data proprietors typically struggle to assert the secrecy and the level of granularity regarding access control for shared data with limited access.

Having said that, it can be difficult to establish precise borders between shared data with limited access and trade secrets as the distinction lies in the purpose, scope and level of confidentiality associated with each concept in each individual case. But as a rule of thumb and in contrast to the concept of shared data with limited access, data with trade secret status is typically not shared or disclosed to anyone outside the organization that owns them and subject to very strict organization-internal access-control schemes, as will be elaborated below with regard to code and algorithms.

To illustrate how important it can be to differentiate between trade secret protection and protection as shared data with limited access, one can consider the following hypothetical example around a proprietary algorithm for optimizing energy consumption in industrial manufacturing processes.

Example of trade secret algorithm and sharing certain data with limited access

Organization A offers and sells energy optimization software. The heart of Organization A's energy optimization software is its proprietary algorithm, which provides a significant competitive advantage in the market. This algorithm is a trade secret that embodies years of research, development and testing.

1 For Japan, e.g., see the Guidelines on Shared Data with Limited Access at: https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/guidelines_on_shared_data_with_limited_access.pdf. See also the EU Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act) at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

Organization A takes extensive measures to keep this algorithm confidential and secure. The company restricts access to the algorithm to a small team of trusted software engineers who have signed strict non-disclosure agreements. The algorithm's source code is stored on secure servers with advanced encryption, and access is granted only on a need-to-know basis. No external parties, including collaborators or partners, have access to the complete algorithm, ensuring that Organization A maintains exclusive control over this valuable trade secret.

Now, Organization A decides to collaborate with a research institution, Organization B, to advance the field of energy-efficient manufacturing. As part of the collaboration, Organization A shares certain data related to manufacturing processes and energy consumption trends with Organization B. However, to protect their intangible assets, Organization A sets up an agreement that limits Organization B's access to specific subsets of data. This limited access allows Organization B's researchers to analyze the data for research purposes only, ensuring that the core proprietary algorithm and implementation details remain confidential and inaccessible. Organization A retains control over the key trade secret – the precise algorithm – which is never shared with Organization B or any other party.

In this example, the shared data with limited access represents a controlled sharing of non-core information with a collaborator, while the trade secret encompasses the core proprietary algorithm, which is kept strictly confidential within the company. Organization A strategically manages the boundaries between shared data and the trade secret to balance collaboration with protection of its most valuable intellectual property.

3.2 Code and algorithms

As mentioned above, code is the language used to write software programs, contains the implementation details of algorithms and can reveal crucial business information about how data is processed and utilized. Unless an open-source strategy is pursued, protecting the confidentiality of code and algorithms is paramount to prevent unauthorized individuals from understanding or reverse-engineering proprietary software in order to build and defend competitive edges over competitors. In practice, techniques such as code obfuscation, encryption, and strict access controls are applied to maintain the confidentiality of code (and the algorithms behind it) and to prevent unauthorized access or copying.

There are some industry-specific implications, but it is generally far less common to share code and/or algorithms between businesses than, for example, sets of processed data. This indicates and emphasizes the commercial value attributed to, and the level of secrecy applied to, code and algorithms and opens a primary playing field for digital data trade secrets.

Copyright is another form of intellectual property protection available to code and algorithms. However, it should be noted that certain jurisdictions do not permit an owner to assert both trade secret and copyright, especially if the copyrighted software discloses a majority of the source code or the "proprietary" portions.[2] In the Capricorn case, the court held that the source code owner was barred from asserting trade secret protection because the code was also registered as a copyright, and thus available to the public. Therefore, the source code owner should carefully consider the pros and cons of each type of protection.

4. Management of digital trade secrets

We have seen that digital objects may be protected by trade secrets (i.e., **digital trade secrets**) as long as they meet the eligibility criteria for such protection. The subsequent question is how the holders of digital trade secrets can properly manage them so that they can prove, in administrative and/or judicial proceedings, that the eligibility for trade secret protection has been met in an individual case.

2 Capricorn Mgm't Sys., Inc. v. Gov't Emps. Ins. Co. et al., 15-CV-2926 (DRH) (SIL) (E.D.N.Y.)

The proper management of digital trade secrets involves defining and categorizing the information to establish its protected status, outlining the necessary measures to continuously safeguard its confidentiality, and developing a trade secret management lifecycle around each or each kind of trade secret. This section is tailored to specific challenges and opportunities surrounding effective management of digital trade secret assets. However, the descriptions relating to technology measures against disclosure and unauthorized use of trade secrets are also applicable to non-digital trade secret information in a digital format.

4.1 Identifying and selecting digital trade secrets

Businesses need to first identify and select specific digital information that qualifies as one or more trade secrets, and clarify which digital object or collection of digital objects defines each respective trade secret.

Capturing digital trade secret information

Assuming that the digital objects are tagged and can be specifically identified, the first step of **capturing potential digital trade secret information** is rather straightforward. It requires the creation, transfer or copying of the relevant digital objects into a dedicated file management system or structure to clearly separate them from non-relevant digital objects (e.g., into a trade secret management system on-premises, in a commercial or corporate cloud storage, encrypted IoT device, to specially designated and locked-away hard drives, or the like).

This step as such can be executed for an individual object or multiple objects at the same time. Batch-captures of multiple objects that require the same set of permission(s) facilitate the person capturing the information, as the metadata of the capturing process is shared across all objects that are recorded in one session and does not have to be provided (often manually) on a per-digital object basis. Under this approach, intake of potential digital trade secrets in a collection can be an automated process while the trade secret status designation is handled by specially trained personnel (e.g., Chief Trade Secret Officers, or trade secret professionals within the IP department) with their own stack of resources or with full automation via API gateway or other file transfer mechanism to a secure storage designation.

It should be noted that the initial capturing step can be done completely anonymously, or it can be combined with the capture by the trade secret creator. The latter may facilitate identifying employees to be rewarded under employee remuneration or incentivization programs.

Designating digital trade secrets

Once the potential trade secret information is captured, it is vital to **designate digital trade secrets**, taking into account the value of the trade secrets and their risks. By clearly defining their scope, businesses can better understand the level of protection required and the strictness of access control.

Examples of workflows for identifying and selecting digital trade secrets

Example 1: Potential trade secret information is captured by an employee

- Employee A uploads Documents 1, 2, 3 and 4 – all related to a specific financial algorithm, e.g., its design document, its user manuals and its source code.
- Decision Maker B reviews the uploaded documents and (e.g., in cooperation with Employee A) designates Documents 1 and 3 as trade secrets that require corresponding access controls.
- Decision Maker B electronically informs Employee A about the trade secret status of Documents 1 and 3, and the non-trade secret status of Documents 2 and 4.

Example 2: Potential trade secret information is captured by an IoT device

- IoT device collects raw process equipment data – all related to a proprietary process.
- IoT device uses an internal algorithm to compile the data and segregate the data that is useful

for further downstream processing.
- IoT device encrypts this segregated data, which is then securely communicated on a routine basis to a separate on-premises server or cloud storage for further use by data scientists. The data scientists are informed that the data in such location are considered trade secrets.

In general, in selecting information to be protected by trade secrets, an over-inclusive approach is preferred compared to a too restrictive selection, since the latter might entail the risk of losing control of information that may later turn out to be critical. However, **excessively inflationary trade secret designation** for any collected information without further review of trade secret eligibility should be avoided in order to: (i) keep the amount of digital trade secret information manageable and well-structured; and (ii) be able to prove that the digital trade secrets are managed in a finely differentiated categorization system and are not simply in a "file dump." Otherwise, a court may not agree with the owner's trade secret claim.[3]

It is important to emphasize at this point that digital information which does not achieve trade secret status in this intermediate step can nevertheless be valuable as contextual information in transactions, since it can facilitate the implementation of trade secrets, e.g., as know-how, and be protected via commercial agreements.

4.2 Timestamping

One of the key advantages of digital trade secrets is the **ability to timestamp** them. Timestamping the contents of documents provides a way to establish the existence, the integrity and the possession of the contents at a specific point in time. Typically, timestamping involves a trusted third party or a centralized timestamping authority who assigns a unique timestamp to the document, which is then digitally signed by the authority, **creating a verifiable proof of the document's existence at that time**. To be precise, the utility of the timestamping is not limited to digital trade secrets but also extends to non-digital trade secrets in a digital format (e.g., a manufacturing process of chemical compound X described in a digital file).

For this purpose, some national or regional intellectual property offices established a service that provides a date- and time-stamped digital fingerprint of any file.[4] While governmental services largely benefit from the trustworthiness of the timestamping authority, digital timestamping is an option that can nowadays be enabled in many commercial data storage solutions.[5] Further, timestamping raw or processed data usually occurs automatically at collection in the form of metadata. However, such timestamping requires this metadata "tag" to be continuously associated with the data. If the link is broken, there is no proof of when the collection occurred.

Blockchain

Blockchain technology can offer a decentralized and tamper-resistant alternative to timestamps from a centralized authority or service.[6] Blockchain-based timestamping involves recording a cryptographic hash of the document into a blockchain, along with the timestamp.

The decentralized nature of blockchain ensures that no single entity has control over the timestamps, making it difficult for anyone to manipulate the data. Additionally, the immutability

3 This frequently occurs with files or emails marked "confidential and proprietary," but in fact are neither. Courts and tribunals do not appreciate these blanket, non-thoughtful assertions. See FormFactor, Inc. v. Micro-Probe, Inc., et al., No. C 10-3095 PJH, 2012 WL 2061520 (N.D. Cal. June 7, 2012).

4 The Korean Intellectual Property Office provides a service called "KIPRIS" (see http://eng.kipris.or.kr/enghome/main.jsp). The service provided by INPI France is called "l'enveloppe Soleau" (see https://www.inpi.fr/proteger-vos-creations/lenveloppe-soleau/enveloppe-soleau). The Benelux Office for Intellectual Property (BOIP) offers a service called iDEPOT (see https://www.boip.int/en/entrepreneurs/ideas/maintain-an-i-depot#:~:text=An%20i%2DDEPOT%20is%20a,together%20with%20others%2C%20for%20example).

5 For example, for AWS S3: https://aws.amazon.com/blogs/big-data/working-with-timestamp-with-time-zone-in-your-amazon-s3-based-data-lake/

6 On the topic of blockchain technologies and IP ecosystems, further reference is made to the corresponding WIPO publication: https://www.wipo.int/export/sites/www/cws/en/pdf/blockchain-for-ip-ecosystem-whitepaper.pdf.

of blockchain ensures that once a document is timestamped, it cannot be altered or removed without detection.

Blockchain-based timestamping also offers transparency, as the timestamped information becomes part of a public ledger (without disclosing the confidential information itself, see Section 4.3, below) that can be independently verified by anyone. This provides a high level of trust and accountability, as the integrity and authenticity of the document can be verified by multiple participants in the blockchain network. Moreover, blockchain-based timestamping systems often come with built-in mechanisms, such as consensus algorithms, to ensure the accuracy and consistency of the timestamps.

4.3 Measures against disclosure and unauthorized access

Capturing trade secret information in digital systems (be it trade secret management systems, cloud or on-premise data storage or timestamping services) can be the source of various security risks which can: (i) destroy the trade secret status of the captured information as a whole; or (ii) provide opportunities for trade secret misappropriation. Accordingly, the protection measures need to be addressed specifically with regard to digital trade secrets. To be precise, the various digital protection measures addressed in this section are also applicable to digital representations of any trade secrets.

Measures against the disclosure of digital trade secrets

One imminent risk when it comes to capturing trade secrets on digital systems (centralized or decentralized) is the **risk of disclosing a trade secret accidentally** to unauthorized persons or even to the public.

Many traditional trade secret management systems are intentionally run on computers without internet connection (e.g., lab computers) or reside on-premises on local servers of corporate customers with very strict access control even on the hardware side (e.g., no USB devices allowed, no other connectivity enabling data transfers like Bluetooth) and extensive security logs. However, current management systems are "always connected," whether it be cloud storage, personal communication device (e.g. cell phone), or IoT device. Accordingly, digital trade secret capturing systems generally face a lot of security due diligence if they involve (especially external) cloud storage, communication links and/or blockchain integration to implementing technical safeguards and obtaining relevant standard certifications.[7]

Two pillars of digital trade secret security are hashing and encryption. Both are cryptographic techniques used to protect data, but they serve different purposes and have distinct characteristics.

Hashing is a one-way process that **converts data of any size into a fixed-length string of characters**, known as a hash value or checksum, e.g., by hashing documents with a SHA (Secure Hash Algorithm) checksum to ensure data integrity and verify the authenticity of files. SHA checksums generate a fixed-length alphanumeric string that uniquely represents the contents of a document. When a document is hashed using SHA, any slight change in the file will result in a completely different checksum. This makes it virtually impossible to tamper with the document without altering the checksum. By comparing the computed SHA checksum of a document with the original checksum, one can quickly determine if the file has been modified or corrupted.

In the above example wherein trade secrets are timestamped using blockchain technology, the document itself is not disclosed to the ledger itself or stored on a digital file storage system (like the Interplanetary File System (IPFS)). Rather, the document hash (representing either an individual file or a collection of digital files – like .zip files) is permanently recorded on the ledger together with the relevant timestamp, effectively avoiding public disclosure of the confidential information while leveraging the benefits of the transparency of a public blockchain. As such, it is not possible to recreate the hashed document based on its checksum. However, conversely, it

7 For example, ISO/IEC 27001; System and Security Controls (SOC) 2 security audits.

is possible to provide evidence that a document with a matching hash was in possession of the person (or blockchain wallet) to whom the timestamped hash can be attributed at the time when the timestamping occurred.

By hashing documents, information can be stored and hashed offline or on-premises while only the hash is recorded and timestamped online. Naturally, document retrieval from the digital system itself is not possible in these instances as only the hash/checksum is disclosed to the digital system.

Encryption, on the other hand, is a two-way process that **converts data into a ciphertext using an encryption algorithm and a secret key**. The primary purpose of encryption is data confidentiality. It ensures that data remains secure and unreadable to unauthorized individuals. Encryption allows the original data to be transformed into an encrypted form, and **it can be decrypted back into its original form** using the corresponding decryption algorithm and the correct key. This is how modern wireless communication devices operate when sending and receiving data.

In practice, timestamping, hashing and encryption can be combined, depending on the level and nature of individual confidentiality requirements that the trade secret holder wants to introduce.

Access-control measures

In addition, access-control measures should be put in place to prevent unauthorized access, disclosure or theft of the trade secret information from digital systems. A minimum standard for such access controls is **2FA (Two-Factor Authentication)**, a security measure designed to add an extra layer of protection to user accounts and systems by requiring users to provide at least two forms of identification or credentials during the authentication process.

2FA, as the name suggests, utilizes two factors for authentication. Typically, these factors include something the user knows (such as a password or PIN) and something the user possesses (such as a mobile device or security token). When logging in, users enter their password as the first factor and then provide the second factor, often a temporary code generated by an authenticator app or received via SMS.

Depending on the required level of protection, **MFA (Multi-Factor Authentication)** can expand on the concept of 2FA by incorporating additional factors beyond the two mentioned above. These additional factors can include something the user is (biometric data, such as fingerprints or facial recognition) or something the user has (such as a physical smart card or a registered device). By combining multiple factors, MFA provides an even higher level of security and reduces the risk of unauthorized access.

Another option for access controls and security is the institution of a secure enclave, which segregates a database or memory portion with enhanced security controls. This can be done on most storage devices and databases (e.g. laptop, server, mobile).[8] For example, most large corporations use Microsoft Office 365 Mobile secure enclave as a way to segregate company data and allow remote access on a mobile device if there is a security issue.[9] Thus, if a mobile device is lost or stolen, corporate IT can remotely disable the enclave and/or delete its data.

4.4 Interoperability

One additional point that should be mentioned in the context of capturing and designating digital trade secrets is the potential requirement for interoperability. Interoperability refers to the ability of different systems or technologies to seamlessly work together and exchange information.

8 https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-enclaves?view=sql-server-ver16.
9 https://learn.microsoft.com/en-us/microsoft-365/admin/basic-mobility-security/set-up?view=o365-worldwide.

In the context of a **trade secret capturing solution**, interoperability is essential for ensuring that the solution can accommodate future transactions, even if those transactions were not initially anticipated. The capturing solution designed with interoperability in mind is capable of integrating and interacting with other systems, platforms or protocols in the future, if necessary. This foresight allows the solution to support various transactions, such as transfers (sale or intra-company transfers after M&A deals), exchanges or smart contract interactions, regardless of the specific ecosystem or technology they operate on.

A lack of interoperability can result in several disadvantages, including increased transaction costs, as businesses may need to employ multiple platforms to handle different aspects of their trade secret operations. In addition, difficulties of validating/proving unsynchronized timestamps can arise, which may make it more challenging to maintain accurate and consistent trade secret capturing records.

5. Digital trade secrets and large language models

The emergence of **large language models**, such as GPT-4 (Generative Pre-trained Transformer 4), has revolutionized natural language processing and generated new opportunities and challenges regarding trade secret protection. These advanced models have the capability to analyze and generate human-like text, making them valuable tools for various applications, including content generation, customer service automation and data analysis. However, businesses must navigate the delicate balance between leveraging the advantages of large language models internally while protecting their trade secrets from unauthorized disclosure. One recent case that made the press in this context involved Samsung employees allegedly leaking confidential data, such as the source code itself for a new program, internal meeting notes and data relating to hardware whilst using ChatGPT to help them with tasks.[10]

To protect trade secrets while utilizing large language models (LLM) internally, businesses should consider adopting various strategies:

1. Focus on **safeguarding the specific inputs or proprietary data**. By keeping confidential information within their control and limiting access to authorized individuals, businesses can lower the risk of exposing sensitive trade secrets to the LLM. This, as outlined above, may involve implementing access controls, encryption and mechanisms to monitor access to the large language model.
2. Adopt techniques such as **data masking or data obfuscation to prevent the direct exposure of proprietary information to the model**. By modifying or anonymizing certain aspects of the data before inputting it into the model, businesses can maintain the confidentiality of trade secrets while still benefiting from the model's language processing capabilities. Careful consideration should be given to the selection and treatment of data to strike a balance between utility and confidentiality.
3. Establish **clear policies and agreements with employees and contractors** involved in utilizing large language models. Non-disclosure agreements (**NDAs**) and confidentiality clauses can outline the responsibilities and obligations of individuals to ensure the protection of trade secrets. Employees should be trained on the importance of maintaining confidentiality, data security best practices and the risks associated with unauthorized disclosure.
4. Consider a **private instance of the LLM (albeit for a fee)**, where there are contractual safeguards with the LLM vendor regarding use and destruction of proprietary data that is uploaded to the model. Note that OpenAI has such a product that allows individuals or corporations to use GPT-4 on a private basis through APIs.

In conclusion, as large language models like GPT-4 become more prevalent, businesses need to strike a balance between leveraging their capabilities and protecting trade secrets. By doing so, businesses can continue to innovate, improve operational efficiency and maintain their competitive edge in an era of advanced language processing technologies.

10 https://www.techradar.com/news/sansung-workers-leaked-company-secrets-by-using-chatgpt.

6. Challenges and risks in protecting digital trade secrets and mitigation strategies

Digital trade secrets can be exposed to a range of specific potential security challenges and risks. This section addresses the most common challenges and risks – and how they can be mitigated at a high level. It may also be relevant to **non-digital trade secret information in a digital format**.

The **general operational and contractual mitigation measures** against trade secret leakage and misappropriation were explained in Part IV: Trade secret management. As illustrated in Part IV, the importance of setting up institutional decision-making structures, document management, logistical measures, education and training of employees, IT measures and contracts with employees and external partners is also applicable to the protection of digital trade secrets.

In essence, once digital trade secrets are leaked or misappropriated, there is a high risk that they cannot be fully recovered. Therefore, **prevention against disclosure and unauthorized access to digital trade secrets in the first place** should be the priority of any trade secret holders.

6.1 Vulnerability to theft, cyber-attacks and data breaches

In the digital age, protecting digital trade secrets presents challenges and risks, particularly in terms of vulnerability to theft, cyber-attacks and data breaches. These threats pose a considerable risk to the confidentiality and integrity of valuable proprietary information, potentially leading to severe financial and reputational consequences for businesses.

One of the primary challenges in protecting digital trade secrets is the heightened **vulnerability to theft**, since they can be easily copied, shared and disseminated. **Cyber-attacks** by sophisticated hackers and cybercriminals can pose another significant risk to the protection of digital trade secrets. In addition, **data breaches** (exposure of sensitive information by unauthorized individuals or hackers who gained access to a company's digital infrastructure) can result in a loss of secrecy and of the entire value of the trade secrets.

Robust security measures, including regular updates and incident response plans, can be implemented to mitigate the risks. At the same time, security measures should be also at the **reasonable level**, similar to any other measures for trade secret protection. The value of the trade secret versus the cost of trade secret protection and the feature of the organization may also need to be taken into account (see Part IV, Section 2.3).

Already highlighted in Part IV, digital trade secrets are also susceptible to a high risk of disclosure or misappropriation by **current and former employees or by external collaborators and business partners** where trade secret information is shared with them. In the digital technology and digital service sectors, global employee mobility, outsourcing arrangements and utilizing offshore resources are part of the daily business in many organizations, which heighten the risk.

To mitigate the risk, the implementation of **access controls** on a **need-to-know** basis, robust **contractual measures, education and training,** and **exit and inbound interviews** are important not only for prevention of misappropriation but also for avoiding contamination with trade secrets held by others (see Part IV, Sections 3.1 and 5.1).

6.2 Exposure during audits

Internal and external audits play a crucial role in ensuring compliance, identifying operational efficiencies and assessing financial performance. However, the process of conducting audits also requires auditors, even when bound by non-disclosure agreements, to have access to confidential information of the businesses to evaluate their financial statements, internal controls and compliance with regulations. This sharing of information raises the risk of trade secret misappropriation or accidental disclosure to unauthorized individuals.

To mitigate the risk of digital trade secret exposure during audits, businesses should establish robust **confidentiality agreements** with auditors, explicitly outlining the scope of information they are authorized to access and defining their obligations regarding trade secret protection. This agreement should also include provisions for the return or destruction of any trade secret information obtained during the audit process. Additionally, implementing **technological safeguards**, such as data encryption, access controls and data trails, can further protect digital trade secrets during audits.

6.3 Retrieving and regaining control of digital trade secret data

Due to their digital availability, once digital trade secrets have been misappropriated or used without authorization, **retrieving and regaining control** over that information becomes a daunting task.

Organizations can take certain measures to address this issue and attempt to mitigate the potential damage. Besides the "traditional" approach to recover digital trade secrets through **legal recourse**, businesses may consider leveraging technology and **digital forensics** to track and retrieve digital trade secrets. This might necessitate working with specialized cybersecurity firms or forensic experts to trace the unauthorized use of trade secrets, identify the locations or systems involved and attempt to regain control over the information. The process may involve employing advanced data analysis techniques, monitoring networks or utilizing forensic tools to trace the movement and storage of the trade secret data.

The success of these efforts largely depends on the sophistication of the unauthorized user, the extent of their activities, and the availability of digital evidence.

Legal and technological measures to retrieve and regain control over the trade secret information may not always guarantee a full recovery. Therefore, it can be only reiterated that **prevention** against disclosure and unauthorized use of digital trade secrets through robust security and contractual measures, employee training etc. remains crucial.

7. Trade secrets vs. other intellectual property rights for digital objects

7.1 Digital objects: trade secrets vs. patents

As explained in Part III: Basics of trade secret protection, most corporations use a strategy of combining patent protection and trade secret protection, considering the advantages and disadvantages of each protection mechanism. In this section, we briefly look into certain aspects that are particularly relevant to digital objects.

Patentability of digital objects

In general, according to patent laws of many countries, data as such, software code as such and mere presentation of information as such, are not considered as inventions that are eligible for patent protection. Similarly, abstract ideas, mathematical methods as such, as well as business or commercial methods as such, are not patent-eligible subject matter in many countries. However, it is not always easy for innovators to draw a clear line between these subjects excluded from patent protection and patentable software- or computer-implemented inventions.

In addition, due to the differences as to how national patent laws and practices regarding the patent eligibility and patentability criteria are applied to digital objects, even if they are seemingly minor, patent applicants may need to tailor their patent applications to meet specific national requirements, which might add complexity and a higher risk of rejections of patent applications.

Such unclarity about the availability of patent protection for these inventions makes it more difficult for innovators in the digital technology and service sectors to decide whether they should protect their creations under the patent system or the trade secret system.

Challenges in software-implemented patent litigation

Evidence of use

With respect to software-implemented inventions, most patent owners do not have direct evidence of infringement at the time of filing a lawsuit, because such direct evidence requires access to the source code of the alleged infringer. Rather, they claim in good faith that a defendant may be infringing the patent, because the outward functionality of the alleged program is similar to the claimed invention. Obtaining the direct evidence is not easy. In some countries, robust discovery procedures permit patent owners to review source code during litigation. Because most defendants consider the source code a trade secret, third-party "escrow" agents review the source code of the alleged infringer. It works in such a way that the third party accesses a static copy of the code and manages access (usually done on-site to restrict printing or copying) of the patent owner and/or its experts.[11] Once the patent owner identifies sections of the source code to be submitted as evidence of infringement, the parties (often with the help of the tribunal) negotiate how such a submission takes place.

Territoriality

As patents are strictly territorial intellectual property rights, if the alleged infringement of certain elements (but not all) of the claimed invention was geographically distributed among different countries, it can give rise to an array of questions during patent litigation, for example:

- if the data is fragmented and stored in multiple locations (in cloud or on-premises)
- if infringement takes place over multiple servers spanning more than one country
- if data is exported to a country with no patent protection options for data "processing," and the processing results are subsequently re-imported for commercial exploitation
- if unauthorized personnel are relocating data (such as on a USB drive) into countries where no patent protection is available or was sought.

These are just some of the challenges when enforcing patents on digital objects. Unfortunately, there is no single answer to address the above questions. If trade secret protection is pursued (potentially also in a mixed strategy together with patents), robust security measures (e.g., 2FA, encryption, breach detection) are the current, best solution to minimize the risks. If any misappropriation or infringement is identified, one should swiftly act, especially if such identification occurred in a territory with a robust rule of law.

Equitable remedies against patent infringement

The availability of equitable remedies, such as injunction, also varies by jurisdiction. If an injunction is issued, the defendant can usually change a few lines of code or rearchitect a database (sometimes easier said than done) to get around the injunction. This can result in an endless game of "whack-a-mole" with the defendant.

7.2 Digital objects: trade secrets vs. copyright

Copyright should be given careful consideration depending on the type of digital objects being protected. For example, copyright protection may be the best solution for audio and video recordings, especially if such recordings are an original work of authorship and/or will be widely distributed.[12] However, raw or processed digital data that is used internally, or selectively shared via contract, may be best suited for trade secrets. Further, certain data may not be copyright eligible if not considered an original work of authorship. Regarding source code and algorithms, certain jurisdictions don't permit an owner to claim both trade secret and copyright protection for source code – thus the owner should consider the pros and cons of such protection.

11 Parties will often enter into a protective order that limits or restricts patent owner's access, especially in a competitor situation.
12 Jurisdictions are currently struggling on how to assign copyright to audio, video, or text generated by LLMs or other generative models. Thus, such generated content should be considered for multiple protection schemes if available.

7.3 Digital objects: trade secrets vs. contract rights

Trade secrets and contract rights should be considered together. In fact, if a third party generates the trade secret data on behalf of the legal owner, there must be some contract in place to establish "reasonable means of protection." When claiming trade secret protection, the trade secret holder most often points to some type of contractual arrangement (such as non-use and/or non-disclosure agreement) with the alleged misappropriator. If the holder fails in asserting trade secret misappropriation, they can most often rely on basic breach of contract as the remedy.

The holder, however, must correctly and separately plead both causes of action. Otherwise, the tribunal may find that if the data is not subject to trade secret, it is also not subject to confidentiality or non-use restrictions. This is why it is paramount that trade secret data is managed separately from mere confidential or proprietary data.

7.4 Mixed protection strategies for digital data

Based on the above, a combination of patent, trade secret and contractual rights is likely the best strategy for technological innovation. Patent protection may be best suited for a unique IoT device, communication protocol or data storage used to collect and transmit the digital data. Trade secret protection is best suited for the algorithm and data itself (raw and processed). Contractual rights are needed if a third party is involved in the collection, processing or sharing of the data. Such a triple approach gives the data owner a wide array of enforcement options.

Annex: Selected reference materials

World Intellectual Property Organization (WIPO)

Trade secrets webpage

https://www.wipo.int/tradesecrets/en/

Frequently Asked Questions: Trade Secrets

Overview of Trade Secret Systems in Certain Countries and Regions

WIPO series: Business Insights in Trade Secret Management

WIPO Lex Database

https://www.wipo.int/en/web/wipolex/index

National and regional laws relating to trade secrets

Paris Convention for the Protection of Industrial Property

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)

WIPO Arbitration and Mediation Center

https://www.wipo.int/amc/en/

De Castro, I. and Gadkowski, A., Confidentiality and Protection of Trade Secrets in Intellectual Property Mediation and Arbitration, in Gerold Zeiler and Alexander Zojer (eds.), Trade Secrets: Procedural and Substantive Issues, 2020, NWV, pp. 79-90: https://www.wipo.int/export/sites/www/amc/en/docs/confidentialitytradesecrets.pdf

Economic studies

Bravo-Ortega, C. and Price Elton, J. J., Innovation and intellectual property rights in the Chilean copper mining sector: the role of the mining, equipment, technology and services firms, Economic Research Working Paper No. 54, 2019: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_econstat_wp_54.pdf

Keisner, C.A., Raffo, J. and Wunsch-Vincent, S., Breakthrough technologies – Robotics, innovation and intellectual property, Economic Research Working Paper No. 30, 2015: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_econstat_wp_30.pdf

Larrimore Ouellette, L., Economic growth and breakthrough innovations: A case study of nanotechnology, Economic Research Working Paper No. 29, 2015: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_econstat_wp_29.pdf

López, A., Innovation and Appropriability, Empirical Evidence and Research Agenda, in "The Economics of Intellectual Property", 2009: https://www.wipo.int/edocs/pubdocs/en/economics/1012/wipo_pub_1012.pdf

Discussion paper on the interplay between patents and trade secrets in medical technologies: https://www.wipo.int/edocs/mdocs/scp/en/wipo_ip_covid_ge_2_22/wipo_ip_covid_ge_2_22_paper.pdf

Database of Intellectual Property Policies from Universities and Research Institutions

https://www.wipo.int/web/technology-transfer/database-ip-policies-universities-research-institutions

National Institute of Industrial Property (INPI), France

Les autres modes de protection - Le secret (webpage): https://www.inpi.fr/comprendre-la-propriete-intellectuelle/les-autres-modes-de-protection

INPI - Guide du Management de la PI pour les business managers (Fiche-Guide n°11 Protéger le savoir-faire de l'entreprise, Fiche-Guide n°12 Constituer des preuves de ses créations et de leur usage): https://www.inpi.fr/le-management-de-la-pi

Court of Appeal of Paris, France

La réparation du préjudice économique: Fiches méthodologiques et glossaire - 3e édition, 2024 (FR)/ Compensation for economic damage: Guidance notes - 3rd edition, 2024 (EN): https://www.cours-appel.justice.fr/paris/la-reparation-du-prejudice-economique

Fiche 9a: Comment gérer la confidentialité et respecter le secret des affaires ? (FR)/Sheet no. 9a: How can confidentiality be managed and trade secrets respected (EN)

Fiche 9b: Comment réparer les préjudices causés par une atteinte au secret des affaires ? (FR) /Sheet no. 9b: How can damage caused by infringement of trade secrets be compensated? (EN)

Ministry of Economy, Trade and Industry (METI), Japan

Unfair Competition Prevention Law webpage: https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html

Handbook for Protection of Confidential Information - Improving Corporate Value, last updated in February 2021 [Full text in Japanese, last updated in February 2024]; available on the Japanese webpage: https://www.meti.go.jp/policy/economy/chizai/chiteki/index.html)

Management Guidelines for Trade Secrets (last updated on January 23, 2019): https://www.meti.go.jp/english/policy/economy/chizai/chiteki/pdf/0813mgtc.pdf

National Institute for the Defense of Free Competition and the Protection of Intellectual Property (INDECOPI), Peru

Guía sobre el uso del 'secreto empresarial' como alternativa para la protección de las innovaciones y el desarrollo empresarial, 2020: https://repositorio.indecopi.gob.pe/handle/11724/7575

Intellectual Property Office of Singapore (IPOS)

Trade Secrets Enterprise Guide, 2022: https://www.ipos.gov.sg/docs/default-source/resources-library/trade-secrets/trade-secrets-guide.pdf

Study on the Protection and Management of Trade Secrets in Singapore, 2021: https://www.ipos.gov.sg/docs/default-source/resources-library/trade-secrets/trade-secrets-public-report-2sept2021.pdf

Spanish Patent and Trademark Office (OEPM), Spain

Protocolo de Protección del Secreto Empresarial en los Juzgados Mercantiles: https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Noticias/2019/2019_11_22_Protocolo_Proteccion_Secreto_Empresarial_en_los_JM.pdf

UK Intellectual Property Office (UKIPO)

The economic and innovation impacts of trade secrets (April 19, 2021), a report delivered by Dr. Nicola Searle on behalf of the IPO: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets

IP Finance Toolkit, 2015: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478929/ip-finance-toolkit.pdf

United States Patent and Trademark Office (USPTO)

Trade secrets/regulatory data protection webpage: https://www.uspto.gov/ip-policy/trade-secret-policy

Intellectual Property Toolkit – Trade secrets: https://www.uspto.gov/sites/default/files/documents/tradesecretsiptoolkit.pdf

Andean Community Justice Tribunal (TJCA)

Jurisprudencia sobre el Secreto Empresarial & Datos de Prueba: https://www.tribunalandino.org.ec/index.php/jurisprudencia/clasificacion_tematica/propiedad_intelectual/propiedad_industrial/secreto_empresarial/

European Commission

Radauer, A., Bader, M., Aplin, T. et al., Study on the legal protection of trade secrets in the context of the data economy – Final report, 2022, European Innovation Council and SMEs Executive Agency: https://data.europa.eu/doi/10.2826/021443

Trade secrets – Managing confidential business information, 2021, Executive Agency for Small and Medium-sized Enterprises: https://data.europa.eu/doi/10.2826/449107

Non-disclosure agreement – A business tool, 2021, Executive Agency for Small and Medium-sized Enterprises: https://data.europa.eu/doi/10.2826/547286

The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs: https://data.europa.eu/doi/10.2873/48055

European Union Intellectual Property Office (EUIPO)

Trade secrets litigation trends in the EU, 2023: https://data.europa.eu/doi/10.2814/565721

The baseline of trade secrets litigation in the EU Member States, 2018: https://data.europa.eu/doi/10.2814/19869

Protecting Innovation through Trade Secrets and Patents: Determinants for European Union Firms, 2017: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf

OECD

Enquiries into Intellectual Property's Economic Impact, 2015, see in particular, Chapters 1 and 4: https://web-archive.oecd.org/2016-03-21/369774-intellectual-property-economic-impact.htm

Schultz, M. and Lippoldt D., "Approaches to Protection of Undisclosed Information (Trade Secrets): Background Paper", OECD Trade Policy Papers, No. 162, 2014: http://dx.doi.org/10.1787/5jz9z43w0jnw-en

International Chamber of Commerce (ICC)

Protecting Trade Secrets - Recent EU and US Reforms, 2019

Handbook on Valuation of Intellectual Property Assets, 2019: https://www.iccgermany.de/wp-content/uploads/2019/10/icc-handbook-valuation-ip-assets-we.pdf

Licensing Executives Society International (LESI)

Special Issue: International Protection of Trade Secrets and Other Confidential Information, LVI, No.2, les Nouvelles, 2021

Sedona Conference publications

https://thesedonaconference.org/publications

The Sedona Conference Commentary on the Governance and Management of Trade Secrets (2023)

The Sedona Conference Commentary on Monetary Remedies in Trade Secret Litigation (2023)

The Sedona Conference Commentary on Cross-Border Discovery in U.S. Patent and Trade Secret Cases ("Stage Two") (2023)The

Sedona Conference Commentary on Equitable Remedies in Trade Secret Litigation (2022)

The Sedona Conference Commentary on Protecting Trade Secrets in Litigation About Them (2022)

The Sedona Conference Commentary on Protecting Trade Secrets Throughout the Employment Life Cycle (2022)

Others

Cook, T. (ed.) (2022). *Trade Secret Protection: A Global Guide* (2nd edition). Globe Law and Business Ltd.

Pooley, J.(1997). *Trade Secrets* (updated edition 2024. Law Journal Press.

Sandeen, S. and Rowe, E. A., (2018). *Trade Secret Law in a Nutshell* (2nd edition). West Academic Publishing.

Aplin, T., Bently, L., Johnson, P. and Malynicz, S. (2012). *Gurry on Breach of Confidence: The Protection of Confidential Information* (2nd edition). Oxford University Press Inc.

In the dynamic and increasingly interconnected world of innovation and commerce, intellectual property (IP) protection plays a pivotal role in driving economic growth, fostering competition and promoting technological advancements.

Among various forms of IP protection, trade secrets have emerged as a critical tool for businesses to safeguard valuable confidential information and to maintain a competitive edge in an increasingly global marketplace.

The *WIPO Guide to Trade Secrets and Innovation* provides a global audience with a comprehensive but digestible strategic and legal overview of trade secrets in the modern innovation ecosystem.