Management for Professionals

Pierre Ollivier
Graham Bell
Victor De Leon
Sylvain Roy *Editors*

Business Secrets Management

Strategies to Protect, Extract and Maximize Value

Springer

Management for Professionals

The Springer series “Management for Professionals” comprises high-level business and management books for executives, MBA students, and practice-oriented business researchers. The topics cover all themes relevant to businesses and the business ecosystem. The authors are experienced business professionals and renowned professors who combine scientific backgrounds, best practices, and entrepreneurial vision to provide powerful insights into achieving business excellence.

The Series is SCOPUS-indexed.

Pierre Ollivier • Graham Bell •
Victor De Leon • Sylvain Roy
Editors

Business Secrets Management

Strategies to Protect, Extract and Maximize Value

Springer

Editors
Pierre Ollivier
Winnotek
Paris, France

Graham Bell
Cubicibuc
Cambridge, UK

Victor De Leon
Accralaw
Manila, Philippines

Sylvain Roy
SRA
Montréal, QC, Canada

ISSN 2192-8096 ISSN 2192-810X (electronic)
Management for Professionals
ISBN 978-3-031-82511-8 ISBN 978-3-031-82512-5 (eBook)
https://doi.org/10.1007/978-3-031-82512-5

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Secrets are often the silent engines of business success. From Coca Cola's recipe and KFC's iconic 11 herbs and spices to Amazon's recommendation engine or Apple's face ID technology, businesses have developed winning products and services by carefully managing their companies' business secrets, e.g. trade secrets, sensitive information, etc. Exclusive access to these valuable assets has enabled corporations to innovate, fund, and deliver transformative solutions — sometimes benefiting society with substantial productivity gains and advancements.

Secrets in the form of formulas, algorithms, composition, and processes have shaped industries, driven innovation, and touched nearly every aspect of daily life. Looking ahead, new technologies protected as trade secrets —including generative AI algorithms, autonomous driving, biologics manufacturing processes, and space innovations like SpaceX's rocket landing systems—promise to drive economic growth, influence national and international politics, and reshape the relationship between citizens, states, and businesses.

Unlike patents which are formalized by disclosure and registration, business secrets remain, by definition, "secret." Their protection relies on meticulous management of employment policies, IT infrastructure, and commercial agreements. A single misstep—a careless disclosure or a lapse in internal controls—can result in the irreversible loss of what may be company's most valuable asset. While resources abound on intellectual property strategies—patents, copyrights, trademarks, and design—there is a notable scarcity of practical guides focused on business secret management. The need for a dedicated management handbook on this subject was clear.

This book on *Strategies to Protect, Extract and Maximize Value* is designed as an accessible yet comprehensive guide for business managers seeking to better understand and use business secrets. It provides actionable insights and strategies for protecting, monetizing, and leveraging confidential information in an increasingly competitive and interconnected world, all by balancing legal and operation considerations.

Authored by a dozen legal and consulting advisors, all members of the Licensing Executives Society (LES), this book draws on the expertise of practitioners at the forefront of innovation and commerce. The idea for this volume originated with our esteemed colleague and co-author, Véronique Chapuis. It is our sincere hope that

this book will illuminate the nuances of business secret strategy and equip readers with the tools to protect and harness these relating invaluable assets effectively.

All the best,

Pierre, Graham, Vic, Sylvain

Paris, France — Pierre Ollivier
Cambridge, UK — Graham Bell
Manila, Philippines — Victor De Leon
Montréal, Canada — Sylvain Roy

Contents

Book Reference Terms, Definitions, and Cases

Graham Bell, Ferzana Haq, Victor De Leon, Pierre Ollivier, Sylvain Roy, and Philippe Simon

Abstract

This book is addressed to business and academic executives and senior managers in small and medium-sized businesses or scale-ups that need to understand how to effectively manage the business secrets within their organisation, particularly during new product launches, finance raising, and mergers and acquisitions (M&A). The book keeps away from technical legal details that are important for legal experts but are not absolutely necessary for managers and executives in their daily lives. It may happen, nevertheless, that some of these terms appear while reading the chapters below, because the authors believed they were necessary to reach some level of understanding the strategic issues concerning business secrets.

The authors also believe that non-legal business executives can grasp the essentiality of these terms and then use them to design and implement

G. Bell
Cambridge, UK
e-mail: graham@cubicibuc.com

F. Haq
Singapore, Singapore
e-mail: ferzanahaq@hslegal.com.sg

V. De Leon (✉)
Manila, Philippines
e-mail: vnlllb@gmail.com

P. Ollivier · P. Simon
Paris, France
e-mail: pierre.ollivier@winnotek.com; philippe.simon@winnotek.com

S. Roy
Montreal, Canada
e-mail: sylvain@sroy.ca

P. Ollivier et al. (eds.), *Business Secrets Management*, Management for Professionals, https://doi.org/10.1007/978-3-031-82512-5_1

comprehensive business secrets strategies for all employees. Moreover, having a foundational understanding of the legal concepts at play will also increase their ability to communicate with companies' legal teams and external advisers.

A number of recent confidential information and secret-related legal cases are believed to be representative of the issues that require attention from managers and executives. These are also summarised in this section. These cases come from small to big size companies and involving multiple industries such as chemicals, drugs, biotechnology, information technology, car fleets, car manufacturing, food technology, pharmacy, admin services, and metal industry.

This section summarises the elements that are useful to refer to when reading its chapters.

1 Glossary of Terms

This section is a summary of the technical terms, concepts, and expressions that are used throughout the book.

"Absence of IP assets from corporate accounting statements": Because intellectual property (IP) assets are intangible, they are usually not grasped by corporate accounting which lacks adequate knowledge and tools to assess a confidence interval for their monetary value. At best, an efficient cost accounting system may allow identification of the historical R&D, engineering, and legal costs incurred while creating the invention and use these as a proxy for the value of the corresponding IP asset; however, a historic sum of costs is seldom a reflection of current realistic monetary value which may be significantly more or less than the sum of costs. Although national reporting standards like the International Financial Reporting Standards (IFRS) now require the reporting of intangible assets, experience shows that in liquidation contexts for example, liquidators value a failing company's IP assets at best at the legal costs incurred for filing and prosecution of patents, trademarks, etc., and at worst value them at zero.

"Breach of confidence": Action by the recipient of confidential information which violates a confidentiality clause applying to said information, whereby said clause restricts the freedom of said recipient to disseminate, share, use, etc., the information. Such clauses typically appear in employment contracts, non-disclosure agreements (NDAs), collaborative projects, and suppliers or subcontractors' agreements.

"Breach of duty of confidentiality": An action whereby the recipient of confidential information violates one or several confidentiality clauses applying to said information spelled out in a contractual agreement the recipient has signed and to which the recipient is legally bound. Whether the violation is unintentional (e.g. negligence) or intentional (e.g. counterfeiting or malevolence) is irrelevant to the materiality of the breach once it is established.

"Burden of proof": In the framework of litigation, it is a responsibility assigned to one party by law or by the court to find and exhibit material proofs, either that their own claim is legitimate or that the other party's claim is invalid or untrue.

"Business secret or Trade secret value estimates": These estimates are heuristical methods used either internally (by the owner of a business secret) or by courts (in litigation contexts) to assign a financial value to the business secret, even though it is not a registered IP asset that is liable to "classical" value estimate methods. Most often, the assigned value is an estimate of the financial damage incurred by the legitimate owner if the business secret is leaked, pilfered, pirated, unlawfully used, etc. The nature of the damage may cover loss of revenues/margins, loss of future sales opportunities, equity losses due to harmed image/reputation, etc. As for all heuristical methods, the assigned value is assessed as a confidence interval, not a single amount.

"Confidentiality clauses": Contractual clauses of an employment contract, NDA, collaborative project agreement, supplier contract, or subcontractor contract, restricting the freedom of recipients of a defined set of data to disclose, share, or use the same, in order to preserve the interests of the legitimate data owner. Recipients may be employees, partners, subcontractors, suppliers, etc. The sets of data covered by the clauses must be spelled out in the contract but may encompass up to 100% of all information labelled as "confidential" by the owner.

"Discovery" and "e-discovery": "*Discovery*" is a legal procedure whereby a court authority orders the seizure of part or all of a company's documents, files, e-mails, etc., relative to an ongoing litigation, so that the court and the opposing party may, through a detailed review and analysis of contents, find and exhibit evidence supporting or invalidating the plaintiff's claims or the defendant's defence. "*E-discovery*" is the method of executing the discovery with the help of IT / AI tools to handle massive, digitalised data and speed up the sorting out of relevant versus irrelevant data, via machine learning (ML) algorithms.

"Document Classification": The process of assigning one or more class or categories to documents created within an organisation. Distinct from indexing which may seek to identify the contents of a document for search purposes, classification typically allocates a label to a document that signifies how the document is to be controlled based on sensitivity and business context. Labelling may use levels of confidentiality such as: Public, Internal, Restricted, and Confidential.

"Dual-use technology": Technology that can be used for both civilian and military purposes in the broader sense.

"FMEA", or "Failure Mode Economic Analysis": A formal method of quality assurance and risk reduction leveraged during design of a product or process. The method identifies how the system, product, or process may fail, and what the most likely consequences would be in terms of performance, user safety, durability, and repair/restoration costs (including catastrophic failure). It assigns probabilities to each failure mode and leads to design or manufacturing process changes in order to minimise these probabilities.

"Gardening leave": A human relations (HR) management practice whereby an employee who resigns or is dismissed remains on the payroll during his advance

notice period but is forbidden from visiting the company's premises or from starting a new job until the advance notice period is exhausted. This method is very rigorously applied in particular by British courts especially when the employee initially refuses to abide by his advance notice period and wishes to leave immediately.

"Good conscience": A state of mind of a stakeholder having access to confidential information, whereby the stakeholder sincerely believes that the way they use said information is lawful, legitimate, and does not harm the interests of the original owner of the confidential information. This commonly signifies that the stakeholder has no conscious intention of causing damage to the original owner, even though they may actually do so (e.g. by negligence).

"Informal or non-registered IP assets": Confidential information that holds value for its owner but does not qualify for registration or for labelling as legally recognised intellectual property (patents, trademarks, designs & models, databases, copyrighted documents, algorithms, and formalised know-how). Business secrets are initially considered "informal IP assets" before they may mature or graduate into formal IP assets.

"Innovation cycle": An outline of the step-by-step process undertaken by organisations to bring new innovations or inventions to life, from idea generation and conceptualisation (in-process assets) to development and execution, and ultimately, protection (formal and identified assets).

"Intangible asset": A non-physical asset such as—but not limited to—a patent, brand, trademark, copyright, trade name, software code, etc.

"Interests served by business secrets": A typology of stakeholders each possessing a vested interest in secrecy protection, or conversely, in the disclosure of a business secret. This typology is usually established in litigation contexts where a plaintiff claims a defendant has unlawfully accessed and/or used a business secret. At a minimum, the typology includes: (a) Interests of the legitimate owner and its shareholders, (b) Interests of competitors, (c) Interest of the end users or the public at large (in the case of a business secret generated within a Public Research Organisation), and (d) "National strategic interest" (secrets relating to defence, diplomacy, strategic resources, etc.).

"Key questions for employees receiving information": A set of questions any employee receiving information labelled as "confidential" should promptly seek answers to. They concern the legitimacy of the person transmitting the information to do so, the legitimacy of the recipient to receive it, the recipient's degrees of freedom (to solely detain the information; to share it with peers; to disclose it to third parties; to use it internally or with outsiders, etc.), the positioning of the information on a secrets classification scale ("fit for disclosure"; "restricted"; "sensitive"; "critical", etc.), and the identity of the other employees competent to give directions to the recipient on how to behave. Ideally, all these questions may be addressed in the company's business secrets policy as taught to all employees once formalised.

"Knowledge management system": A system utilised by an organisation or entity to keep track of, manage, and protect, among other things, their internal

business and trade secrets and confidential and sensitive information. When properly utilised, it protects the confidentiality of the information it contains.

"Need to know basis": A rule governing the dissemination of confidential information within an organisation or towards its business partners. It generally states that any employee, regardless of hierarchical level, seniority, or function, is only allowed to access, hold, and use specific confidential information if that information is required for him to efficiently perform his daily duties or other duties specific to a given project he is assigned to. (E.g., a sales manager may be prevented from accessing the detailed cost structure of a product whereas the lower ranking design technician in charge of "target costing" may be allowed access to such information in order to perform his job.)

"Open data environment": A movement originating in the United States of America (USA) and the United Kingdom (UK) which aims to promote and generalise online disclosure by public sector stakeholders (government agencies, state and local administrations, PROs, universities, etc.) of part of their own databases for the benefit of the public at large.

"Open science": The movement that aims to make scientific research, data, code, and publications freely accessible to everyone without barriers.

"Open source": Originally coined for software, Open source promotes universal access via open-source licenses. Software source code, which is typically released under the terms of an open source software license, may generally be downloaded and modified, and then published back to the community (sometimes mandatorily with the same licensing terms).

"Open standards": A standard that is openly accessible and usable (be implemented) by anyone. Open standards may have open source obligations, but not all do.

"Public disclosure": These are certain business secrets that may already be publicly available or have been previously disclosed.

"Reverse engineering (RE)": A method whereby a research and development (R&D) department or a laboratory breaks down a product or system into its primary components to identify its bill of materials and to understand its design and the technical explanation of its features and performances. The same method applies to analysing a machine or manufacturing system to understand and reconstitute each step of a manufacturing process in order to identify the technical innovations leading to its level of performance as expressed by a set of key progress indicators (KPIs).

"Sensitive information": Intermediate grade on a classification scale for business secrets, above "restricted" and below "critical". Its leakage or capture may cause serious damage to the company but may not harm it to the point of liquidation, unlike "critical" business secrets. Symmetrically, leakage of "restricted" business secrets may cause damages which are non-trivial but are usually controllable and are not lethal.

"Strategic information": Confidential information with commercial value that competitors do not have access to. Such information must also be kept confidential with some legal, contractual, digital, and safety protection measures.

"Unauthorised use": An action by the recipient of information labelled as "confidential" (or explicitly labelled as a business secret) that infringes the explicit restrictions binding the recipient, either through contractual confidentiality clauses or as spelled out in the company's business secrets protection policy. This may include the recipient sharing the information whereas they are only authorised to hold it, using it without explicit clearance from their hierarchy, disclosing it to outsiders, using it for other purposes than their professional duties warrant it, or using it malevolently to serve personal interests and/or harm the firm (such as leaking it to a competitor, e.g.)

"Undisclosed information": This means information that fulfils three conditions stated in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS): "(1) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (2) it has commercial value because it is secret; and (3) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret".

"Wrongful gain/loss": "*Wrongful gain*" is a quantifiable and/or qualitative gain achieved by the recipient of confidential information (by leveraging this information in various ways), where said information was obtained by unlawful means and leveraged without explicit authorisation from the original owner of the information. "*Wrongful loss*" is symmetrically the quantifiable and/or qualitative damage incurred by the original legitimate owner of the information due to the fact that a third party detains and uses said information without his authorisation and against his will.

2 A Few Definitions to Keep in Mind

"Business secret" is here defined as any information that (1) is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to persons familiar with this type of information because of their sector of activity; (2) has commercial value, actual or potential, by virtue of its secrecy; (3) is the subject of reasonable protective measures by its legitimate holder, given the circumstances, to maintain its secrecy.

In other words, a business secret: (1) must be known within the organisation, (2) must not be known to anyone outside the organisation, and (3) results in loss of value to the organisation and / or gain in value to the external entity *if leaked.*

If a piece of information meets all three of these criteria, it should be considered a business secret.

Of course, the second test can be modified to "it must not be known to anyone outside the organisation in the absence of suitable legal obligations such as NDAs"—but this is a topic that will be covered extensively in this book.

"Trade secret" would usually be more rigorously defined as a piece of information that passes the three following tests:

1. It is not known to the professional sector or field of activity concerned. (i.e., *it is not naturally or effortlessly accessible to stakeholders of the trade who would, in the course of their professional duty, want or need to access it*)
2. It is valuable in view of the fact that the information is secret (i.e., *it can be assigned a commercial value, explicit or latent)*
3. The company endeavours to keep it secret by taking reasonable protective measures (i.e., *its legitimate owner has already enforced specific protection measures to preserve secrecy*)

"Sensitive information" has different meanings in various contexts. It may mean both:

- A catch-all word that designates in practice any confidential information or data that is important to a company because it is relevant for its business and
- Depending on jurisdiction, a precise word with significant meaning. For example, in France, it is used in the Protection of the Scientific and Technical Heritage of the Nation (PSTH, PPST in French) and the Blocking Act of 1968,[1] revised by the Decree of 22 February 2022(**).

The interest in qualifying the information a company possesses is to know one's rights and obligations but also the value one can generate from such information, according to the operational context. For example, if confidential information is considered "sovereign sensitive" in the sense of the Blocking Act,[2] it cannot be communicated to foreign authorities.

Therefore, in this book, Trade secrets or a sensitive information are business secrets, but the reverse may not be true, specifically due to differences in national laws around the world.

3 Examples Showing Key Situations and Issues Behind Business Secrets

This section outlines cases that show how decisions related to confidential information have developed in today's worldwide economic environment. They represent examples demonstrating key scenarios and issues introducing the importance of business secrets management.

[1] Law 68–678 of July 26, 1968 relating to the communication of documents and information of an economic, commercial, industrial, financial, or technical nature to foreign natural or legal persons.

[2] Decree n° 2022-207 of February 18, 2022 relating to the communication of documents and information of an economic, commercial, industrial, financial, or technical nature to foreign natural or legal persons. The SISSE (Service de l'information stratégique et de la sécurité économiques du Ministère de l'Économie et des Finances) provides explanations (https://sisse.entreprises.gouv.fr/fr/actualites/accueil/loi-de-blocage-revision-des-modalites-et-publication-d-guide-d-aide).

3.1 Case 1: Kolon

Full name: **E.I. Dupont De Nemours & Company v. Kolon Industries Incorporated** (United States).

Facts	Subsequent decision	Main takeaways for management
Facts: Dupont produces Kevlar fibre. Kolon was in the same business when it sought five (5) former Dupont employees to work as consultants to improve its product. Through the new employees, Kolon obtained information regarding the manufacturing process of Kevlar. Dupont sued Kolon. Kolon wanted to introduce evidence to show that some of Dupont's trade secrets were publicly available information as they appeared in the records of an earlier intellectual property case between Dupont and another competitor. Dupont objected to Kolon presenting evidence or arguments concerning another case.	The court ruled that a new trial is warranted in order to give Kolon an opportunity to prove its theory that the alleged trade secrets are in fact publicly available information.	1. Implement protective actions to prevent leakage such as (a) listing the key information to be protected, in a document signed by the employee by the time he/she leaves, and (b) identify potential claims by the company against a former employee as well as the duration of the validity of these potential claims. 2. Trade secrets presented as evidence in a prior litigation may later be classified as publicly available information. 3. Information released to government authorities (i.e. courts during litigation) should be treated and reviewed carefully in light of a clear trade secret IP strategy.

3.2 Case 2: Hytera

Full name: **Motorola Solutions, Inc, et. Al. v. Hytera Communications Corp. Ltd.** (United States).

Facts	Subsequent decision	Main takeaways for management
Facts: Hytera hired Motorola engineers who gave the former more than 10,000 technical documents downloaded from Motorola's database which were used by Hytera on a product similar to that of Motorola. Motorola sued Hytera et al. for trade secrets misappropriation and copyright infringement.	The jury decided in favour of Motorola, and Hytera's subsequent motions for judgment as a matter of law and for a new trial were denied. The court disagreed with Hytera's assertion that Motorola "*failed to satisfy the elements of a trade secret claim" and "failed to use*	1. Put in place minimum reasonable protection measures such as (a) having employees sign confidentiality agreements and (b) classifying and storing trade secrets in a database with limited and controlled access from employees. 2. Including non-compete clauses in employee contracts

(continued)

Facts	Subsequent decision	Main takeaways for management
	reasonable security measures to protect its secrets".	may also be a good protection measure. 3. Employees should be made aware of the consequences of stealing trade secrets.

3.3 **Case 3:** Waymo

Full name: **Waymo LLC v. Uber Technologies** (United States).

Facts	Subsequent decision	Main takeaways for management
Facts: Mr. Levandowski resigned from Waymo and started his own self-driving vehicle company called Otto. Mr. Levandowski then was suspected of having taken with him, together with other Waymo employees who joined him at Otto, confidential information about Waymo's LiDAR technology. Otto was bought by Uber who investigated former Waymo employees (which led to a report called "the Stroz report"). Waymo sued Levandowski and Uber for patent infringement and trade secret violation.	A settlement agreement was reached.	1. Be aware of unusual pre-separation activities, which give rise to an inference of misappropriation of business secrets. 2. Consider imposing activity restrictions on employees intending to move to competitors. 3. Consider requiring new employees to confirm in writing that they have completed a thorough analysis of their possessions and returned any confidential information to their former employer. 4. When illicit information is suspected within the company, do not dispose of it but call legal experts to address the problem. 5. Consider having a plan of action where something is suspected, including doing potential early forensic investigations.

3.4 **Case 4:** Dohme

Full name: **Merck Sharp & Dohme Corp. v. Pfizer Inc. et al.** (United States).

Facts	Subsequent decision	Main takeaways for management
Facts: Dr. Wendy Watson, an employee of Merck, had access to confidential	The court partly granted and denied the motions of both parties.	1. Be conscious of unusual use of business secrets access through discreet

(continued)

Facts	Subsequent decision	Main takeaways for management
information on Merck's vaccine programme. Dr. Watson left Merck and worked at Pfizer in a similar position. Merck filed a case for trade secrets misappropriation against Pfizer and Dr. Watson, claiming that after an investigation was conducted, it was found that before Dr. Watson left, she downloaded thousands of documents prior to her departure, copied them, and transferred them to her devices and Pfizer's computers. Both parties aimed to compel the other to disclose specific information on their own cases to each other.	On the issue of trade secrets, the court stated that a business pursing a trade secret suit must "identify its trade secrets *with a reasonable degree of precision and specificity that is particular enough as to separate the trade secret from matters of general knowledge in the trade or of special knowledge of persons skilled in the trade*". In other words, trade secrets must be "identified with sufficient particularity so that the reader understands how each such claim differs from public domain information-including public patent filings".	investigations, specially for departing employees who had access to such. 2. This practice may be standardised and carried out on a regular basis across all employees who have access to a company's business secrets. 3. Formulate a precise description of your trade secrets such that they are distinguishable and distinct from public information.

3.5 Case 5: Wyeth

Full name: **Wyeth v. Natural Biologics Inc.** (United States).

Facts	Subsequent decision	Main takeaways for management
Facts: Wyeth developed the "Brandon Process" for making conjugated oestrogens used in Premarin. Natural Biologics sold conjugated oestrogens. It used an extraction process that yielded material which was the same as Premarin. Natural Biologics claims to have independently developed its process through a review of Wyeth's expired patents, scientific literature, and Wyeth's Brandon Facility waste manifests, which reveal the names and volumes of chemicals used at the	The court ruled that Wyeth had implemented reasonable efforts to maintain the secrecy of the Brandon Process, given the following: *The lack of repeated losses of confidential information regarding the Brandon Process, the use of physical security, limited access to confidential information, employee training, document control, and oral and written understandings of confidentiality.* Additionally, the court ruled that that since no one had previously duplicated the	1. Put clear indications that certain information is (a company's) secret. 2. Make it a practice to manage and protect business secrets relating to manufacturing processes for as long as possible as this may give rise to future business secrets. 3. Be aware of the synergy between patents and business secrets.

(continued)

Facts	Subsequent decision	Main takeaways for management
Brandon Facility. It was contended that Wyeth did not adequately protect its trade secret.	Brandon Process, it is unlikely that Natural Biologics had succeeded in doing so legally.	

3.6 Case 6: Coco

Full name: **Coco v A.N. Clark (Engineers) Ltd [1969] RPC 41** (United Kingdom).

Facts	Subsequent decision	Main take aways for management
The plaintiff (Coco) shared confidential information with the defendant (A.N. Clark Engineers Ltd.) in the course of negotiations for a potential business collaboration to manufacture a new motor scooter engine. The negotiations fell through, but the defendant later produced a similar product. Plaintiff claimed that the defendant had used his confidential information in the production process. Plaintiff sought an injunction to prevent the defendant from using the confidential information, alleging a breach of confidence.	The court established a three-part test to determine the existence of a breach of confidence: (1) The information must be confidential in nature and possess the necessary quality of confidentiality (i.e. it must not be public knowledge). (2) The information must have been communicated in circumstances importing an obligation of confidence. (3) There must be an unauthorised use of the information to the detriment of the party who communicated it. The High Court ruled that the defendants were not in breach of confidence, as there was no unauthorised use of the plaintiff's confidential information. Although the information was shared in circumstances that imposed an obligation of confidence, the court found insufficient evidence of misuse in the production of the defendant's product. The case did not progress to the court of appeal, further to the plaintiff arguing that the High Court took a too narrow view of unauthorised use.	1. Ensure that the information you seek to protect qualifies as confidential. Clearly identify this information as confidential through documentation and reference disclosure of such information in your confidentiality agreements. 2. Be explicit about the confidential nature of disclosed information and ensure that all parties involved understand their non-disclosure and non-use obligations. 3. Document any case of unauthorised use and collect evidence that the information was used without permission or that unauthorised use caused harm or a competitive disadvantage. 4. Improve your confidentiality agreements. Explicitly outline the recipient duties and ensure these agreements are legally enforceable in the event of a breach. 5. Develop strategies to monitor and enforce the proper use of confidential information. This includes tracking the flow of sensitive information within and

(continued)

Facts	Subsequent decision	Main take aways for management
	This judgment remains influential in trade secret law, particularly in cases where confidential information is shared during business negotiations, but no clear evidence of misuse or damage can be proven. It highlights the importance of demonstrating actual harm from unauthorised use when pursuing a claim for breach of confidence.	outside the company, especially during negotiations, collaborations, or employee departures.

3.7 **Case 7:** Clearlab

Full name: **Clearlab SG Pte Ltd v Ting Chong Chai and others [2015] SLR 163** (Singapore).

Facts	Subsequent decision	Main takeaways for management
The plaintiff Clearlab, a Singaporean company, had employees who signed an express confidentiality clause. The employees resigned and subsequently went into a business with another party to set up a competing business in the field of production of contact lenses.	The court applied the three-part test used in the *Coco* case and held that all three elements were present: (1) The primary defendants were former Clearlab employees and were therefore under an implied obligation of confidentiality and good faith during their employment. However, they were also obliged to keep Clearlab's information confidential post-employment because of an express confidentiality clause in their employment agreements. (2) The third-party recipient of the information (who was not a former employee) was also bound by an equitable obligation of confidence, because the documents containing the information were marked as confidential, and that he had objective	1. There should be express confidentiality clauses in employment agreements that cover both the period of employment and post-employment. 2. Information should be marked as confidential to ensure that any third-party recipients have objective notice of confidentiality and are therefore bound by an equitable duty of confidence. 3. Wide confidentiality clauses are enforceable and can protect any information of the company which is not public information. However, the express confidentiality clause cannot be relied upon to restrict a former employee from using his skill and knowledge. There may be practical issues in assessing and distinguishing information that is skill and

(continued)