
RISK MANAGEMENT FOR TRADE SECRETS AS CORPORATE ASSETS UNDER INDIAN LEGAL FRAMEWORK

Aishwarya K, Advocate

ABSTRACT

Trade secrets are intellectual property of conditional nature. Their protection is dependent on demonstrable steps taken to preserve their secrecy, existence of duty of trust between the parties who are privy to the trade secrets and proof these two conditions. This is different from other statutory monopolies and these conditionality makes them commercially fragile. This paper argues this instability of trade secrets which stems not from their inherent nature but from their dependency on governance framework.

This study reconceptualises trade secrets from an intangible asset to a risk-exposed corporate capital by examining judicial practices, and economic theories like appropriability and information cost theory. The structural vulnerabilities associated with trade secrets are identified to assess the threat of asset durability even before litigation.

The central claim advanced through this paper is that the commercial value of trade secrets can be increased or retained not through litigation but through structured practical framework as part of governance mechanism. This is categorised across different stages and circumstances in which trade secrets are commercially exploited including but not limited to method of dissemination of information and documentation infrastructure. This reframing of trade secrets as corporate assets of commercial value exposes the probability of profit maximisation of this unique intellectual property within Indian Commercial Practice.

Keywords: Trade Secrets; Confidential Information; Appropriability; Evidentiary Burden; Risk Management; Asset Value

I. INTRODUCTION TO TRADE SECRETS AS CONDITIONAL INTELLECTUAL PROPERTY

A. The Historical Emergence of Trade Secret Protection

The evolution of trade secret protection did not originate as an intellectual property statute. Other IP, like Patents trace their lineage in sovereign grant of monopoly in Europe during the Renaissance, but trade secrets evolved through principles of equity and commercial morality. In Earlier English Courts, while dealing with confidential, non-public information stated that even in the absence of explicit contract, breach of confidence would exist as principles of equity would not permit any person to act unconscionably in abusing an information that has been imparted in trust.¹ Thus secretive information was protected based on the ingenuity attached to it and the effort undertaken to protect the same and this was more relational relying on duty of confidence than proprietary.

In *E.I. du Pont de Nemours & Co. v. Masland*, Justice Holmes famously observed that the “word property as applied to trade secrets, is an unanalyzed expression,” and that the primary fact is that the law expects the rudimentary requirements of good faith.”² This formulation captured the doctrinal ambiguity that has followed trade secret law for over a century. Protection arose not from state-certified exclusivity, but from the equitable maxim that equity will restrain the breach of confidence.³

The 19th and early 20th centuries witnessed the gradual absorption of trade secrecy into unfair competition doctrine in the United States and Breach of Jurisprudence in common law systems. The formalisation of trade secret protection was done by The Restatement (First) of Torts (1939) which defined trade secret as information that derives independent economic value from not being generally known and is subject to reasonable efforts to maintain secrecy.⁴ Later, this was codified in Uniform Trade Secrets Act (UTSA) as a dual requirement: economic value plus reasonable secrecy precautions.⁵

Internationally, trade secrets achieved formal recognition under Article 39 of the TRIPS

¹ See *Saltman Eng'g Co. v. Campbell Eng'g Co.*, (1948) 65 RPC 203 (Ch.).

² Accord *E.I. du Pont de Nemours & Co. v. Masland*, 244 U.S. 100, 102 (1917).

³ See *id.*; Dr. Pauline Sadler, Protection of Confidential Information in the Engineering Industry, 7 The Eng'g Ind. (2005), <https://classic.austlii.edu.au/au/journals/LegIssBus/2005/4.pdf>

⁴ Restatement (First) of Torts § 757 (Am. L. Inst. 1939).

⁵ Uniform Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985).

Agreement, which obliges member states to protect undisclosed information against unfair commercial use, provided that such information is secret, has commercial value, and has been subject to reasonable steps to keep it a secret.⁶ The significance of this TRIPS formulation lies in the fact that it entrenches conditionality at the multilateral level. Protection is not automatic; it is contingent upon secrecy of the information and precautions taken to protect the same.

B. From Relational Obligation to Conditional Intellectual Property

Scholars' discussion on the concept of trade secrets have oscillated between property theory and relational obligations arising from contractual arrangements. Some argue that trade secrets is at the conjunction of incentive theory, unjust enrichment principles and everyday commercial morality and therefore lacks any coherent justificatory framework.⁷ On the other hand, it has been contended that since trade secrets encourage innovation and channel inventors towards patent disclosure wherever appropriate, they must also be treated as intellectual property rights.⁸ However, even pro-IP scholars acknowledge that the inherent nature of trade secret being a secret acts as a gatekeeping mechanism thus demarcating narrower boundaries.

The defining structural feature of trade secret protection is conditionality. This means that the protection of trade secret will only subsist as long as the condition of secrecy is maintained. And the exclusive protection would cease as soon as it is disclosed. Such disclosure may be accidental, voluntary or even through independent discovery. This is in contrast to other IP exclusive rights, like patent which depends upon the grant of patent but once granted the rights persist for the fixed statutory term.⁹ Moreover in trade secrets, when the exclusivity ceases it cannot be restored or remedied because the very essence i.e condition of secrecy doesn't exist anymore.

The information-cost theory sheds light on the difference between remedial and constitutive approaches of law when it comes to trade secret exclusivity. According to this theory, information is treated as a commodity and since it cannot be distributed equally, it has certain costs associated with it and decision makers usually operate within set boundaries where

⁶ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr.15, 1994, 1869 U.N.T.S. 299.

⁷ Robert G. Bone, A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 Cal. L. Rev. 241, 245, 266, 284 (1998).

⁸ Mark A. Lemley, The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 Stan. L. Rev. 311, 313–15 (2008).

⁹ *Id.* At 336–39.

they can access or process such information without indulging in excessive costs and therefore settle for ‘satisfactory’ outcomes instead of ‘perfect’ choices. This compromise defines the modular boundaries that are set for third-party interactions.¹⁰ When patents and copyright subject matter can be disclosed to the public without any exclusion, it can still enjoy protection because of such disclosure even. But in case of trade secrets, transactional boundaries define the extent of secrecy and thus the boundaries are privately construed and invisible to public and it is upon the right-holder to not only safeguard but also prove the adequacy of such modular boundaries for maintaining the trade secret a secret.

This structural design of trade secrets shifts risk internally. Where statutory IPs depend upon statutory recognition and setting up boundaries, trade secrets have no such provision. So the maintenance burden of defining boundaries and safeguarding it is internalised within the corporate body or few individuals. The requirement of “reasonable efforts” to preserve secrecy ensures that protection is only granted to the holder when he has actively constructed the protective measures and necessary safeguards were put in place.¹¹ Trade Secrets are therefore not merely informational assets; they are governance-dependent conditional assets.

C. The Position of Trade Secrets within the Global Legal Framework

In the global context, trade secrets currently occupy a hybrid position within intellectual property systems. They further informal appropriation mechanisms for patents in fast moving industries for purposes of maintaining commercial secrecy, competitive-lead and time advantages and even to prevent replication. In industries where reverse engineering is difficult or where disclosure would undermine competitive advantage, corporates may prefer retaining the information as a trade secret rather than obtain patent through disclosure. At the same time, the absence of registration and time limits renders trade secrets protection as potentially perpetual, but perpetuity is illusory if secrecy collapses.

The European Union’s Trade Secrets Directive (2016) similarly imposes conditional protection based on secrecy, commercial value and reasonable steps.¹² Therefore the convergence of TRIPS, UTSA, and EU standards demonstrates that modern trade secret law is universally structured around conditional entitlement. Protection is predicated upon secrecy

¹⁰ Henry E. Smith, *Intellectual Property as Property: Delineating Entitlements in Information*, 116 Yale L.J. 1742, 1751–68 (2007).

¹¹ Bone, *supra* note 7, at 277–82.

¹² Directive (EU) 2016/943 of the European Parliament and of the Council, 2016 O.J. (L 157) 1.

and precautionary measures and not mere authorship or invention.

This conditionality directly impacts asset classification. In accounting terms, 'asset' is a resource controlled by an entity from which future economic benefits are expected to flow. Trade secrets can satisfy this definition only as long as control is maintained. Loss of secrecy undermines the control and consequently, economic value. This feature is unique to informational assets because they don't retain value after physical intrusion like tangible assets but stands to suffer irreversible dissipation upon disclosure.

D. The Indian Recognition Frameworks of Trade Secrets

In India, there is no statute dedicated to trade secrets. Their protection arises primarily through equitable doctrines of breach of confidence and contractual arrangement under the Indian Contract Act, 1872. In *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*,¹³ the Delhi HC recognised that confidential technical know-how developed through effort and investment is entitled to protection against unauthorised use. Similarly, in *Burlington Home Shopping Pvt. Ltd. V. Rajnish Chibber*,¹⁴ the Court acknowledged that customer databases and proprietary business information may constitute protectable confidential information.

It can be inferred that Indian Courts have accepted the conceptual legitimacy of trade secrets. However, they have consistently emphasised that protection depends on confidentiality and that general skills and knowledge acquired during employment remain unprotected.¹⁵ The entitlement is relational and conditional and not absolute.

Therefore, Indian jurisprudence also aligns with the global framework of secrecy, commercial value and reasonable efforts and these three form the tripartite basis of trade secret protection. Yet, in the absence of statutory demarcation, the burden of defining and maintaining the boundaries of trade secret protection rests heavily on the claimant.

The cumulative effect of historical development and global concurrence of the doctrinal structure establishes the uniqueness of trade secrets within intellectual property. They are:

¹³ *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987 SCC OnLine Del 372.

¹⁴ *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber*, 1995 SCC OnLine Del 401.

¹⁵ *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638.

- a) Recognised as legally protectable interests
- b) Able to generate significant economic value
- c) Subsisting indefinitely

Yet, their existence is fragile needing constant vigilance on secrecy. The maxim *ubi jus ibi remedium* operates imperfectly when it comes to trade secrets. Remedies may restrain misuse, but they cannot reconstruct secrecy once destroyed.

II. THE INDIAN LEGAL STRUCTURE ON RECOGNITION OF TRADE SECRETS AND THEIR STABILITY

A. Doctrinal Groundings without Statutory Codification

Intellectual Property in India like Patents, Trademarks or Copyrights all have a comprehensive legislative framework governing them but not trade secrets. The protection of trade secrets in India arises through a composite consisting of contractual enforcement and equitable principles of breach of confidence and injunctive relief under the Specific Relief Act, 1963.¹⁶ The absence of codification doesn't per se mean absence in protection rather it situates trade secrets within judge-made law or rather precedents.

The Bombay High Court in *Zee Telefilms Ltd. V. Sundial Communications Pvt. Ltd.*¹⁷ Acknowledged the protection of confidential information and trade secrets against unauthorised disclosure or misuse based on equity and obligations arising from contract rather than statutory monopoly. It also emphasised that confidentiality arises when information is imparted in circumstances that imported the obligation of confidence.

Similarly, the Delhi High Court in *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*¹⁸ Restrained the misuses of technical know-how that had been developed through labour and investment. It held that when a party receives confidential information, they cannot exploit such information to the detriment of the confider. Still, the court did not characterise this information as property in the strict proprietorial sense. The court's purview was

¹⁶ Specific Relief Act, No. 47 of 1963.

¹⁷ *Zee Telefilms Ltd. v. Sundial Commc 'ns Pvt. Ltd.*, 2003 SCC Online Bom 344.

¹⁸ *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987 SCC OnLine Del 372.

on misuse and breach of confidence rather than on absolute dominion.

B. Judicial Identification of Confidential Information

Indian Courts have repeatedly insisted on the parties to establish that whatever information had been brought in question qualifies as confidential. Protection is not applicable for vague or general claims of secrecy.

The Delhi Court in *Burlington Home Shopping Pvt. Ltd. V. Rajnish Chibber*¹⁹ recognised customer database as a confidential information provided it was developed through substantial effort and was not in public domain and it has accrued commercial value from such secrecy. The distinction between information readily accessible by others and information compiled through proprietary effort was clarified by the Court, the later qualifying as confidential kind.

The Calcutta High Court in *Hi-Tech Systems & Services Ltd. V. Suprabhat Ray*²⁰, the court examined whether information lost its confidential character when technical know-how was disclosed during the course of employment. The court restrained the misuse only where secrecy was demonstrable. This decision underscored that mere existence of knowledge doesn't suffice; the information must be specific, identifiable and confidential in fact.

In *Desiccant Rotors International Pvt. Ltd. V. Bappaditya Sarkar*²¹, the Delhi High Court emphasised on two conditions: the first being identification of the confidential information; the second being proof of proprietary nature of the information. Courts are therefore reluctant to protect amorphous categories such as “business strategies” or “general expertise” unless concretely delineated.

From these cases, it can be inferred an implicit judicial test as follows:

- a) The information must be specifically identified.
- b) It must not be public knowledge or easily ascertainable.

¹⁹ *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber*, 1995 SCC OnLine Del 401

²⁰ *Hi-Tech Systems & Services Ltd. v. Suprabhat Ray*, 1996 SCC OnLine Cal 331

²¹ *Desiccant Rotors Int'l Pvt. Ltd. v. Bappaditya Sarkar*, 2009 SCC OnLine Del 1258.

- c) It must possess commercial value by virtue of secrecy.
- d) It must have been disclosed in circumstances importing confidence.
- e) There must be actual or threatened misuse.

These elements are cohesive with international formulation under TRIPS, yet they are derived through the common law in India rather than legislatively. The burden of satisfying each element rests upon the claimant.

C. Precaution and Proof: Conditionality in Practice

The Courts of India while scrutinising evidence related to protection of trade secrets, apply a precautionary requirement similar to “reasonable efforts” terminology used in Uniform Trade Secrets Act, although it is not explicitly adopted.

In *Navigators Logistics Ltd. v. Kashif Qureshi*²², the Delhi High Court examined the measures taken by the plaintiff to preserve confidentiality of client details and logistics data which was claimed to be a trade secret and whether they were concrete enough including restricted access and contractual safeguards. It also assessed whether the information was treated internally as confidential, thereby linking enforceability to organisational conduct.

Similarly, in *Diljeet Titus v. Alfred A. Adebare*²³, the Court restrained former employees from utilising client lists and proprietary information, but only after being satisfied that the information was indeed confidential and not merely part of professional skill. Court while analysis looked toward the existence of confidentiality agreements and restricted dissemination which influenced the decision.

The Bombay High Court in *VFS Global Services Pvt. Ltd. V. Mr. Suprit Roy*²⁴ recognised the proprietary character of certain internal databases but examined the manner in which such information was protected within the organisation.

These cases collectively demonstrate the courts evaluation of not just the nature of the information but also the conduct of the claimant. Courts hesitate to grant injunctive relief where

²² *Navigators Logistics Ltd. v. Kashif Qureshi*, 2018 SCC OnLine Del 10369.

²³ *Diljeet Titus v. Alfred A. Adebare*, 2006 SCC OnLine Del 1368.

²⁴ *VFS Global Services Pvt. Ltd. v. Mr. Suprit Roy*, 2008 SCC OnLine Bom 497.

the plaintiff cannot demonstrate vigilance through documentation, access control, or contractual clarity. The maxim *vigilantibus non dormientibus jura subveniunt* finds practical expression in this context. Thus the condition of secrecy need demonstrable effort to prove its existence.

D. Structural Restraints of Employee Mobility and Section 27 of ICA, 1872

The fragile nature of trade secret protection in India is amplified by Section 27 of the Indian Contract Act, 1872 which renders agreements in restraint of trade void, subject to only certain narrow exceptions.²⁵ It was held by the Supreme Court in *Superintendence Co. Of India (P) Ltd. V. Krishnan Murgai*²⁶ that post-employment restraints are generally unenforceable. Also, in an earlier judgement, the Court upheld that the negative covenants which were operative during the subsistence of employment would be invalid if they were to extend beyond the employment except in cases where statutory exceptions are provided.²⁷ This was also reaffirmed in *Percept D'Mark (India) Pvt. Ltd. V. Zaheer Khan*²⁸ where the SC stated post-contractual non-compete clauses are void unless they fall within statutory exceptions.

High Courts have reconciled these principles with trade secrets protection by distinguishing between general skill and proprietary confidential information. In *American Express Bank Ltd. V. Priya Puri*²⁹, the Delhi High Court declined restraint of employee from using general expertise but recognised protection of clearly defined trade secrets.

Indian public policy strongly favour labour mobility. Trade Secrets enforcement must therefore find doctrinal equilibrium by operating within narrow confines protection secrecy without imposing unlawful restraint. This is another factor contributing to the conditional character of the trade secret entitlement.

E. Remedies and Limits of Judicial Restoration

Relief sought in trade secrets disputes are mostly in the form of interim and permanent injunctions under the Specific Relief Act. Courts apply the traditional triad: prima facie case,

²⁵ Indian Contract Act, No. 9 of 1872, § 27.

²⁶ *Superintendence Co. Of India (P) Ltd. v. Krishan Murgai*, (1980) 4 SCC 427.

²⁷ *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co.*, (1967) 2 SCR 378.

²⁸ *Percept D'Mark (India) Pvt. Ltd. v. Zaheer Khan*, (2006) 4 SCC 227.

²⁹ *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638.

balance of convenience, and irreparable injury.³⁰ In *Gujarat Bottling Co. Ltd. V. Coca Cola Co.*,³¹ the Supreme Court emphasised that preservation of status quo pending adjudication would be the governing principle in interim injunctions arising from contracts.

In trade secrets disputes, such injunctions may restrain further misuse, however once information enters the public domain, restoration of secrecy is often impossible. Damages although theoretically available are notoriously difficult to quantify given that the loss consists of not just measurable revenue diversion but also competitive advantage.

Therefore, judicial remedies are reactive with respect to protecting trade secret infringement and not reconstructive. Even if further misuse is restrained, informational exclusivity stands dissipated.

III. RISK ARCHITECTURE OF TRADE SECRETS AS VULNERABLE CORPORATE ASSETS

The legal recognition of trade secrets and their doctrinal conditionality and enforcing difficulties manifests within corporate structures as a series of risk exposures that threaten the economic value of trade secrets even prior to litigation. Thus there's a need for mapping structured assets risk architecture as follows:

A. Design Risk: Boundary Instability and Definitional Failure

The lack of unique statute to govern trade secrets have resulted in lack of definition of what constitutes as trade secrets itself, resulting in a lack of clearly demarcated exclusion boundary like that of patents. Hence, trade secrets solely depend upon secrecy rather than registration and therefore the boundaries are constructed by the organisation. The firm must decide upon what all constitutes as proprietary information, how it is stored, who can access it and what can be the disclosure protocols. When the trade secrets fails to qualify any of these checklists, they cease to function as a stable asset even before it goes to the courtroom.

The risk of collapse in the internal architecture defined by the organisation would include whether confidential and non-confidential information are commingled; whether documentation is present in writing and binding; whether the access controls are formal or

³⁰ Specific Relief Act, No. 47 of 1963, §§ 36 – 42.

³¹ *Gujarat Bottling Co. Ltd. v. Coca Cola Co.*, (1995) 5 SCC 545.

informal, etc... Over and above these conditions the organisation must also maintain an internal register of proprietary information without which the perimeter of exclusivity would dissolve automatically. If there is discrepancy in any of these mechanisms or at any stage, the loss is not merely evidentiary but also structural, because then the informational asset would become indistinguishable from general corporate knowledge.

Judicial reasoning also only looks at the measures taken, as it doesn't construct secrecy but only assess whether secrecy was maintained.³² But practical vulnerability precedes adjudication. Possibility of containment of secrecy diffusion would become impossible in the following cases:

- a) Sharing of information across departments
- b) Transmission without confidentiality markings
- c) Accessibility through unrestricted digital systems

In these scenarios, even if litigation succeeds later, the competitive advantage is lost due to informational dissipation.

Design risk therefore arises at the level of boundary architecture and reflects the absence of modularisation i.e the failure to create controlled compartments of access and documentation. In Asset Management terms, this is equivalent to failure of fencing a physical property. Thus the entitlement's fragility is not court imposed but rather embedded on the asset's dependence upon governance.

B. Relational Risk: Human Interfaces and Appropriability Failure

Where design risk raised concerns at the construction phase, relational risks examines the boundary permeability at points of human interface. Trade Secrets can rarely remain confined within a single individual or department. Their commercial utility depends upon their circulation within network of employees, consultants, vendors, and strategic partners. Each such relational node introduces exposure.

³² See e.g., *Navigators Logistics Ltd. v. Kashif Qureshi*, 2018 SCC OnLine Del 10369 (examining the claimant's conduct in maintaining confidentiality).

Unlike tangible assets, informational assets are non-rivalrous in consumption but rivalrous in appropriation. Once the information is disclosed beyond controlled boundaries, the asset may be replicated without diminishing the holder's physical possession, yet its economic exclusivity may be irreversibly compromised.³³ This phenomenon is called the classical appropriability problem: the difficulty of capturing returns from innovation when information is easily transmissible.³⁴

In situations where § 27 of the Indian Contracts Act, 1872 favour labor mobility such as the limits on post-employment restraints, the risk of enforcing proprietary entitlements are amplified especially in information-intensive industries, particularly in circumstances where tacit knowledge and trade secrets are difficult to separate.³⁵ Courts too protect trade secrets but refuse to restrain general skill or professional advancement.³⁶

The value of an intellectual property lies in its capacity to generate supra competitive return through exclusion. Where this exclusion becomes uncertain (due to migration of information through relational networks), the expected value of the asset declines. This depreciation of value is not always sudden; it may occur gradually through information diffusion, reducing competitive lead time rather than eliminating secrecy entirely.³⁷

Thus, the more the circulation of information within collaborative networks the greater the risk of appropriability failure and consequently economic depreciation.

C. Evidentiary Risk: Proof Failure and Asset Devaluation

Evidentiary risk dismantles the collapse of enforceability when there is inadequate proof. Trade Secret protection is not self-executing. It must be demonstrated and the burden of proof lies upon the claimant who had to establish the existence, scope, secrecy, and misuse of

³³ James Y. Stern, Intellectual Property and the Myth of Nonrivalry, 99 Notre Dame L. Rev. 1163, 1179–1200 (2024).

³⁴ See generally Nicola Searle, *The Economic and Innovation Impacts of Trade Secrets*, U.K. Intell. Prop. Off. (2021), available at <https://research.gold.ac.uk/id/eprint/30022/1/The%20Economic%20and%20Innovation%20Impacts%20of%20Trade%20Secrets%20published%20version.pdf>

³⁵ Paulina Korycińska-Rządca, Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets Against Unauthorised Acquisition, Use and Disclosure by Its Employees?, 29 Białostockie Studia Prawnicze 163, 167–69 (2024).

³⁶ *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638.

³⁷ Christopher Buccafusco, Jonathan S. Masur & Deepa Varadarajan, Trade Secrecy's Information Paradox, 100 Notre Dame L. Rev. 925, 930 (2025).

the information at issue.³⁸ This evidence structures possess document failure as an asset failure.

The requirement of reasonable precautions also serves a dual function: it filters opportunistic claims and incentivises the organisation to take up the cost of maintaining secrecy.³⁹ However this filtering mechanism also produces fragility. When the steps taken for precautionary conduct is informal, undocumented, or inconsistently applied, the organisation may not be able to satisfy judicial scrutiny even if the information is commercially available.

Indian courts also exemplify this evidentiary conditionality in multiple cases where along with nature of the information, the organisational behaviour of the claimant was also assessed.⁴⁰ Likewise, Court granted protection only when the information had been specifically identifiable and was subjected to confidentiality obligations.⁴¹

Therefore it is significant to note that trade secret becomes indistinguishable from general business knowledge when it is poorly documented, in evidentiary terms. Courts cannot enforce what cannot be delineated. Apart from this, evidentiary risk reflects the cost of verification. The enforcement of intellectual property entails adjudicative costs which can influence the scope and reliability of the protection.⁴² When the proof is complex, uncertain or difficult to prove, the enforcement value declines.

This evidentiary burden is more pronounced in digital environments. Contemporary corporate information systems generate metadata, access logs, and digital trails that may either strengthen or weaken the claims of confidentiality. Failure to restrict access, eg. Audit access for the proprietary data increases the probability of court declaring them as insufficiently protected. Conversely, systematic protocols for logging and access can be used not only to secure the confidentiality of the information to be protected but also to later prove such protection and function as evidentiary assets. Empirical Studies on the rise of trade secret litigation further illustrates that disputes frequently arises from internal governance failures rather than external espionage.⁴³

³⁸ See *Desiccant Rotors Int'l Pvt. Ltd. v. Bappaditya Sarkar*, 2009 SCC OnLine Del 1258.

³⁹ Bone, *supra* note 7, at 262–70.

⁴⁰ *Navigators Logistics Ltd. v. Kashif Qureshi*, 2018 SCC OnLine Del 10369.

⁴¹ *Diljeet Titus v. Alfred A. Adebare*, 2006 SCC OnLine Del 1368.

⁴² Korycińska-Rządca, *supra* note 35.

⁴³ David S. Almeling, Four Reasons to Enact a Federal Trade Secrets Act, 19 Fordham Intell. Prop. Media & Ent. L.J. 769, 776–78 (2009).

Thus, evidentiary risk transforms the organisation's laxity into legal vulnerability. The trade secret's commercial value depends not only upon its intrinsic economic utility but also upon the corporate's capacity to prove adequate measures to retain exclusivity. Where proof collapses, enforcement collapses and subsequently the asset value depreciates.

D. Enforcement Risk: Temporal Delay and Irreversibility of Informational Loss

Enforcement risks concerns how judicial protection is reactive in nature. Relief becomes available only after misappropriation is detected or credibly threatened. This temporal structural limit makes it easier for information dissemination.

Of the traditional triad satisfaction for the courts to grant interim injunction,⁴⁴ irreparable injury is often presumed in disputes involving trade secrets on the grounds that loss of confidentiality cannot be easily quantified.⁴⁵ Yet, this very premise reveals the structural fragility that is inherent making restoration of secrecy practically impossible.

Also, Informational Assets are infinitely replicable at negligible marginal cost. Disclosure to a single competitor may enable rapid duplication, market entry or strategic adjustment. Even when injunction restrains further use, the competitive "head start"⁴⁶ gained through initial exposure may not be fully reversible.⁴⁷ Indian Courts have also occasionally recognised this asymmetry by granting time-bound restraints to neutralise unfair advantage.⁴⁸ However, this relief is subjected to evidentiary and temporal limits.

Preventive Relief through interim or permanent injunctions can also be sought from Court as provided under the Specific Relief Act but even such measures does not confer mechanisms to reconstruct the lost status of exclusivity.⁴⁹ Quantifying damages becomes difficult where the injury consists of lost opportunity, diminishing bargaining power, or erosion of first-mover advantage, etc... apart from direct revenue diversion. The informational harm is

⁴⁴ *Gujarat Bottling Co. Ltd. v. Coca Cola Co.*, (1995) 5 SCC 545.

⁴⁵ *See John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987 SCC OnLine Del 372. (Recognising potential irreparable harm from misuse of confidential know-how).

⁴⁶ *Seager v. Copydex Ltd.*, [1967] R.P.C. 349 (C.A.).

⁴⁷ *Winston Research Corp. v. Minnesota Mining & Mfg. Co.*, 350 F.2d 134 (9th Cir. 1965).

⁴⁸ *See e.g., Diljeet Titus v. Alfred A. Adebare*, 2006 SCC OnLine Del 1368. (granting injunctive relief to restrain misuse of proprietary client information).

⁴⁹ Specific Relief Act, No. 47 of 1963, §§ 36–42. Cf. Patents Act, No. 39 of 1970, § 108 (providing statutory remedies including injunction and damages).

often diffuse and manifests as an increased risk of future injury.

The speed of such informational diffusion happens at a rate faster than such disputes can be adjudicated. Also, in cases where litigation extends over months or years, the competitive landscape may also shift irreversibly. Therefore the expected value of enforcement keeps declining the longer it is out in the public.

This temporal restrictions also impedes with evidentiary burden. When there is delay in initiating proceedings, claims of urgency or irreparable harm are weakened. Enforcement risk is therefore not merely a function of judicial reluctance but is embedded in the nature of information itself. The law can restrain misuse but it cannot rewind disclosure. The fragility of entitlement therefore persists even after successful litigation.

E. Transactional Risk: Disclosure Through Commercial Exchange

The economic value of trade secrets are heightened frequently during moments of corporate transaction like mergers and acquisition, technology transfers, joint ventures, strategic alliances, and venture capital investment. Ironically, it is precisely in these moments of maximum valuation, the exposure risk also intensifies. Due diligence processes require disclosure of proprietary information to potential counterparts, often prior to definitive agreement.⁵⁰

Transactional risks are different from relational risks arising out of employment contexts, in that these extend the perimeter of the structural design of trade secrets in every disclosure happening only within structured commercial exchange. In relational risks, the disclosure is subject to non disclosure agreements and the contractual safeguards operate ex post. But, here, there is no agreement of disclosure in the preliminary stage; only after the sensitive technical or strategic information has been reviewed, the possibility of an NDA comes into picture. But, the risk of replication, strategic imitation, or subtle market repositioning to secure the competitive lead persists even when there is no overt breach.⁵¹

Although Indian courts recognise the duty of non-disclosure and confidentiality

⁵⁰ Christopher K. Larus & Rajin Singh Olson, Protecting Trade Secrets During Corporate Transactions, *Financier Worldwide Mag.* (Jan. 2019), <https://www.financierworldwide.com/protecting-trade-secrets-during-corporate-transactions#>

⁵¹ Alan Schwartz & Robert E. Scott, Precontractual Liability and Preliminary Agreements, 120 *Harv. L. Rev.* 661 (2007).

obligations in commercial transactions, the enforcement of the same remains fact-intensive where existence of trade secret is questioned, then, the secrecy and steps taken to secure it were examined and only after any such breach has occurred, courts can take cognisance only after the fact and hence it is reactive.⁵² But in transactional settings, proof may be complicated by layered access structures, shared repositories, or indirect dissemination through independent contractors and sometimes even outsiders accessing through either authorised or unauthorised channels.

Thus, transactional risk reflects asymmetry in information exchange. The very compulsion on organisations to reveal proprietary assets to secure an investment or partnership also reduces exclusivity. The disclosure acts oxymoronic in that they are necessary to further capital generation or other collaborative innovation but simultaneously this disclosure also dilutes the control over information. The trade secret becomes a negotiable asset whose valuation depends on controlled exposure.

Moreover, even in cases where the negotiations fail, residual knowledge would remain with the counterparty. Even without *scienter*, competitive advantage may erode over time on an incremental basis. Litigation in these circumstances become particularly complex, as proving misuse distinct from independent development becomes difficult.

Transactional risks therefore represent a structural paradox: the more a trade secret becomes commercially valuable, the more likely it must be disclosed in order to realise that value. The act of monetisation itself introduces vulnerability.⁵³

IV. CONCLUSION: FINDINGS AND RECOMMENDATIONS

Findings

The following findings emerge from the foregoing analysis:

First, the recognition of trade secrets in Indian Legal framework arises from Article 39 of TRIPS Agreement mandating India to protect “undisclosed information” since it is a signatory to it. But, requirement to protect confidential information as a matter of fair practice

⁵² See *Zee Telefilms Ltd. v. Sundial Commc'ns Pvt. Ltd.*, 2003 SCC Online Bom 344 (recognising enforceability of confidentiality obligations arising from commercial dealings).

⁵³ Buccafusco et al., *supra* note 37.

was introduced by WTO precursor, GATT. Anyhow, protection of trade secrets itself depends upon common law doctrines like Breach of Confidence, Springboard Doctrine, and other contractual and equity obligations and even fiduciary duty when interest of the company is involved. Article 10bis of Paris Convention mandates member nations to provide effective protection against unfair competition which includes misappropriation of trade secrets. Thus, trade secret protection doesn't arise from a single dedicated statutory framework, although an attempt for a sui generis framework was recommended by the 22nd Law Commission of India (Report No. 289) through the Protection of Trade Secrets Bill, 2024, which is currently pending.

Second, the primary tool for trade secret protection is through non-disclosure agreements and non-compete clauses in employment contract. But Indian labour mobility doctrine, particularly under Section 27 of the Indian Contract Act, bars post-employment restrictions and such agreements are held void unless they specifically target trade secret disclosure. The law protects clearly defined trade secrets but refuses to restrain general skill, knowledge, or post-employment competition beyond narrow limits. Thus trade secret protection is conditionally reliant on existence of secrecy along with proof of the same and the considerable steps undertaken to protect the same. Attempt to prove every step results in information dissemination and thus dissipation of economic value of the trade secret.

Third, judicial remedies operate reactively and are temporally constrained. For example, criminal breach of trust and misappropriation remedies can be sought through §§ 316–319 of BNS, 2023. Whereas Copyright Act, 1957 § 13 protects trade secrets that are in the form of programs or databases or technical drawings that come under the ambit of literary work. Protection of digitally stored trade secrets is done through § 72 and §§ 66 & 66E of Information Technology(IT) Act, 2000 which penalises breach of confidence through authorised and unauthorised channels. However these can be triggered only after the misuse has been occurred. Injunctive relief through §§ 36–42 of the Specific Relief Act, 1963 can also be sought but interim injunctions may restrain further misuse, but informational disclosure is often irreversible. Damages are difficult to quantify due to the irreparable injury to competitive advantage.

Fourth, the absence of a codified statutory regime embeds onus of proof, documented evidence on precautionary measures as conditions within the enforcement architecture. This conditionality manifests within corporate structures as design risk, relational risk, evidentiary

risk, enforcement risk, and transactional risk, all of which result in deterioration of the commercial value of the confidential information. Trade secrets therefore function as governance-dependent assets whose durability in the commercial sense depends upon the institutional architecture rather than mere legal recognition.

Collectively, these findings establish that trade secret protection in India is not deficient; it is structurally conditional. The preservation of commercial value cannot be deferred to litigation. It must be engineered ex ante. The conditional nature of trade secrets necessitates structured governance.

Recommendations

The following recommendations are derived directly based on the risks identified in the previous chapters:

1. Trade secret governance requires intentional setting of boundary limitations that can be proved.

This entails:

- a) Institutional classification of proprietary information and imposition of explicit tiered confidentiality obligations;
- b) Maintenance of an internal trade secret register identifying scope, origin, and custodianship;
- c) Modular segregation of confidential and non-confidential information within digital and physical systems;
- d) Periodic audit mechanisms to reassess the status, relevance, and protection of trade secrets as proprietary assets.

2. Trade secret governance requires calibrated dissemination.

This includes:

- a) Limiting access to information based on the Role of the Person and the Necessity for Disclosure;

- b) Confidentiality covenants in non-compete clauses having narrow scope with predefined criteria for informational asset classification as trade secret aligned with Section 27 constraints;
- c) Structured onboarding and exit protocols incorporating confidentiality reaffirmation;
- d) Implementing methods for lawful garden leave and non-solicitation arrangements that protect secrecy without imposing unlawful restraint;
- e) Layered confidentiality protection mechanisms imposed on persons with access like vendors, consultants, and collaborators.

3. Trade secret governance requires documentation-dependent architecture.

This necessitates:

- a) Digital access logging and audit trails;
- b) Confidentiality markings with time stamped version control protocols;
- c) Written acknowledgments at points of access and disclosure;
- d) Secure storage systems with access hierarchy;
- e) Incident documentation and response registers.

4. Trade secret governance requires anticipatory enforcement strategy.

This includes:

- a) Pre-formulated litigation response protocols in the form of pre-stipulated contractual remedies;
- b) Immediate evidence preservation mechanisms upon suspected breach not limited to injunctive relief;
- c) Measures for seeking confidential pleadings and sealed proceedings to prevent further disclosure during litigation.

5. Trade secret governance requires staged and controlled disclosure in commercial transactions.

This involves:

- a) Gradual release of information to comply with due diligence;
- b) Clean room protocols limiting exposure to segregated teams and acting as proof for independent development;
- c) Escrow-based or conditional access to core proprietary assets by signing a tripartite agreement between the Owner, Recipient and a Neutral agent;
- d) Post-transaction certification of destruction or return of sensitive materials;
- e) Layered non-disclosure frameworks binding advisors and intermediaries.

Conclusion

The Indian legal framework on the subject of trade secrets is neither weak nor absolute. It insists on the identification of the confidential information, the nature of secrecy if it exists and the reasonable steps taken to protect the same. This boundary architecture converts the weakness of definition into the strength of evidence. Classification of trade secrets converts the strength of enforcement into the strength of structure. The goal is far from the restriction of trade and mobility, which is allowed. But the aim is the restriction of the migration of trade secrets into competing firms. Structured dissemination of trade secrets converts the weakness of appropriation into the strength of compliance. Courts insist on evidence in the case of trade secrets. Documents convert the strength of precaution into the strength of action. The asset has to be always ready for evidentiary substantiation. Informational assets have an inherent tendency to depreciate in the flow of time. Thus, Loss of informational assets is irreversible. Time converts into an asset depreciation multiplier and Governance converts time into the strength of structure. Therefore structured monetization of trade secrets converts the weakness of capital access into the strength of compliance and enables to retain and even increase the commercial value of this intangible asset thus furthering competitive exploitation to maximise profits.

BIBLIOGRAPHY

A. Primary Sources

Indian Statutes

1. Indian Contract Act, No. 9 of 1872.
2. Specific Relief Act, No. 47 of 1963.
3. Patents Act, No. 39 of 1970.
4. Bharatiya Nyaya Sanhita, No. 45 of 2023.
5. Copyright Act, No. 14 of 1957.
6. Information Technology Act, No. 21 of 2000.

International Instruments

1. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299.
2. General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194.
3. Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 828 U.N.T.S. 305.
4. Directive (EU) 2016/943 of the European Parliament and of the Council, 2016 O.J. (L157) 1.
5. Uniform Trade Secrets Act (Unif. L. Comm'n 1985).

Soft Law

1. Restatement (First) of Torts § 757 (Am. L. Inst. 1939).

Legislative Materials

1. Protection of Trade Secrets Bill, 2024 (India) (proposed legislation).

Case Laws

1. *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638.

2. *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber*, 1995 SCC OnLine Del 401.
3. *Desiccant Rotors Int'l Pvt. Ltd. v. Bappaditya Sarkar*, 2009 SCC OnLine Del 1258.
4. *Diljeet Titus v. Alfred A. Adebare*, 2006 SCC OnLine Del 1368.
5. *E.I. du Pont de Nemours & Co. v. Masland*, 244 U.S. 100 (1917).
6. *Gujarat Bottling Co. Ltd. v. Coca Cola Co.*, (1995) 5 SCC 545.
7. *Hi-Tech Systems & Servs. Ltd. v. Suprabhat Ray*, 1996 SCC OnLine Cal 331.
8. *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*, 1987 SCC OnLine Del 372.
9. *Navigators Logistics Ltd. v. Kashif Qureshi*, 2018 SCC OnLine Del 10369.
10. *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co.*, (1967) 2 SCR 378.
11. *Percept D'Mark (India) Pvt. Ltd. v. Zaheer Khan*, (2006) 4 SCC 227.
12. *Saltman Eng'g Co. v. Campbell Eng'g Co.*, (1948) 65 RPC 203 (Ch.).
13. *Seager v. Copydex Ltd.*, [1967] R.P.C. 349 (C.A.).
14. *Superintendence Co. of India (P) Ltd. v. Krishan Murgai*, (1980) 4 SCC 427.
15. *VFS Global Servs. Pvt. Ltd. v. Suprit Roy*, 2008 SCC OnLine Bom 497.
16. *Winston Research Corp. v. Minnesota Mining & Mfg. Co.*, 350 F.2d 134 (9th Cir. 1965).
17. *Zee Telefilms Ltd. v. Sundial Commc'ns Pvt. Ltd.*, 2003 SCC OnLine Bom 344.

B. Secondary Sources

Books

1. Nicola Searle, *The Economic and Innovation Impacts of Trade Secrets* (U.K. Intell. Prop. Off. 2021).

Book Chapters

1. Herbert J. Hovenkamp, Intellectual Property and Competition, in *Research Handbook on the Economics of Intellectual Property Law* 221 (Peter S. Menell, Ben Depoorter &

David B. Schwartz eds., Edward Elgar 2019).

Journal Articles

1. Robert G. Bone, A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 Cal. L. Rev. 241 (1998).
2. Christopher Buccafusco, Jonathan S. Masur & Deepa Varadarajan, Trade Secrecy's Information Paradox, 100 Notre Dame L. Rev. 925 (2025).
3. Mark A. Lemley, The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 Stan. L. Rev. 311 (2008).
4. Paulina Korycińska-Rządca, Trade Secrets in the Digital Age: How Do the Measures Provided for in EU Law Face the Challenges of Protecting an Employer's Trade Secrets Against Unauthorised Acquisition, Use and Disclosure by Its Employees?, 29 Białostockie Studia Prawnicze 163 (2024).
5. Alan Schwartz & Robert E. Scott, Precontractual Liability and Preliminary Agreements, 120 Harv. L. Rev. 661 (2007).
6. Henry E. Smith, Intellectual Property as Property: Delineating Entitlements in Information, 116 Yale L.J. 1742 (2007).
7. James Y. Stern, Intellectual Property and the Myth of Nonrivalry, 99 Notre Dame L. Rev. 1163 (2024).
8. Pauline Sadler, Protection of Confidential Information in the Engineering Industry, 7 The Eng'g Ind. (2005).
9. David S. Almeling, Four Reasons to Enact a Federal Trade Secrets Act, 19 Fordham Intell. Prop. Media & Ent. L.J. 769 (2009).

Professional Articles

1. Christopher K. Larus & Rajin Singh Olson, Protecting Trade Secrets During Corporate Transactions, *Financier Worldwide Mag.* (Jan. 2019).