ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Volume 13 Issue 06 June 2026

Approaches Towards Trade Secret Protection: A Comparative Study of India and International Jurisdictions

[1] Dheeraj K P, [2] Shobha Yadav

[1][2] Amity Law School, Amity University Bengaluru, India
Email: [1] dheeraj.p@s.amity.edu, [2] syadav@blr.amity.edu

Abstract*— *In today's competitive and technology-driven business environment, trade secrets have become an important asset for companies across the world. Confidential business information such as formulas, business strategies, customer data, and manufacturing processes plays a major role in maintaining commercial advantage. At the same time, the rise of corporate espionage, cyber threats, and unauthorized disclosure of confidential information has increased the need for effective legal protection of trade secrets. This research paper examines the approaches towards trade secret protection in India and compares them with the legal frameworks followed in selected international jurisdictions such as the United States, the United Kingdom, and the European Union.

The study is based on a doctrinal and comparative research methodology. It analyzes laws, judicial decisions, international standards, and policy measures relating to trade secret protection in different jurisdictions. The paper particularly studies the statutory protection available under the United States Defend Trade Secrets Act and the European Union Trade Secrets Directive, while also examining the legal position in India, where protection is mainly derived from contract law, equity, and judicial interpretation.

The research finds that countries like the USA and members of the European Union have developed clearer and more structured legal systems for the protection and enforcement of trade secrets. In contrast, India still lacks a specific legislation dedicated to trade secret protection, which creates uncertainty in enforcement and remedies. The paper highlights the need for a comprehensive legal framework in India that balances international standards with domestic business needs. The study aims to contribute to discussions on improving intellectual property protection and strengthening business confidence in India.

Index Terms*— *Trade Secrets, Corporate Espionage, Comparative Law, Intellectual Property, Legal Protection

I. INTRODUCTION

"Three may keep a secret, if two of them are dead." — Benjamin Franklin[1].

Benjamin Franklin's observation aptly captures the importance and vulnerability of confidential information. In the modern knowledge-driven economy, trade secrets have become one of the most valuable assets of businesses, often rivaling or even exceeding the value of patents, copyrights, and trademarks. Their significance lies not in public disclosure but in maintaining secrecy, which provides enterprises with a competitive advantage in increasingly dynamic and technology-driven markets.

Broadly, a trade secret refers to any confidential business information that derives commercial value from not being generally known or readily accessible. Such information may include manufacturing processes, formulas, algorithms, customer and supplier data, marketing strategies, sales methods, and distribution techniques. Some of the most prominent examples of trade secrets include the Coca-Cola formula, Kentucky Fried Chicken's secret recipe, and Google's search algorithm. The continued success of these enterprises is closely linked to their ability to preserve the confidentiality of such information[2].

With the growth of digital technologies, globalization, and knowledge-based industries, the risk of corporate espionage, cyber theft, and unauthorized disclosure of confidential information has increased substantially. Consequently, effective legal protection of trade secrets has become a critical concern for governments and businesses alike. However, approaches to trade secret protection vary significantly across jurisdictions due to differences in legal traditions, economic priorities, and intellectual property policies.

This paper undertakes a comparative study of trade secret protection in four major jurisdictions—India, the United States, the United Kingdom, and the European Union. While the United States has developed a comprehensive statutory framework through dedicated legislation, the United Kingdom primarily relies on common law principles and contractual obligations. The European Union has sought to harmonize protection through the Trade Secrets Directive, whereas India continues to depend largely on contractual remedies, equitable principles, and judicial precedents in the absence of a dedicated trade secret statute[3]. By examining

[1] Benjamin Franklin, *Poor Richard's Almanack* (1735).
[2] David S. Almeling et al., A Statistical Analysis of Trade Secret Litigation in Federal Courts, 45 Gonz. L. Rev. 291, 292–95 (2010).
[3] 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

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Volume 13 Issue 06 June 2026

these diverse approaches, the study seeks to evaluate the effectiveness of existing legal frameworks and identify lessons that may strengthen trade secret protection in India.

- The main goals of this study are to undertake a comparative analysis of the legal frameworks governing trade secret protection in India, the United States, the United Kingdom, and the European Union, with particular emphasis on their statutory provisions, judicial interpretations, and enforcement mechanisms.
- To evaluate the adequacy of the existing Indian legal framework and propose recommendations for the development of a comprehensive trade secret protection regime that aligns with international standards while addressing India's commercial and technological needs.
- To identify best practices and effective legal principles from the trade secret regimes of the United States, the United Kingdom, and the European Union that may serve as useful models for strengthening trade secret protection in India.

II. INTERNATIONAL OBLIGATION

The protection of trade secrets has become an important aspect of international intellectual property law due to the growing economic value of confidential business information. At the international level, the primary framework for such protection is provided by Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which obligates member states to protect undisclosed information against unauthorized acquisition, use, or disclosure.

The term "trade secret" is not expressly mentioned in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [4] . However, Article 39(1) imposes an obligation on member states to protect undisclosed information. The expression "undisclosed information" is broad and neutral in nature, encompassing trade secrets, confidential business information, as well as commercial and technical information[5]. Article 39(1) establishes the general principle governing the protection of undisclosed information, while Article 39(2) specifies the conditions that such information must satisfy and identifies the acts against which protection must be provided. In addition, Article 39(1) requires the protection of data submitted to governments or governmental agencies, with the scope of such protection further elaborated under Article 39(3). Therefore, Article 39(1) lays down the overarching framework for the protection of undisclosed information and data submitted to governmental authorities, which are subsequently regulated in paragraphs 2 and 3.

Article 39 of the TRIPS Agreement reads:

"Article 39.1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices10 so long as such information:

(a) 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;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

(footnote original) 10 For the purpose of this provision, "a manner contrary to honest commercial practices" shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

III. LEGAL FRAMEWORK FOR TRADE SECRETS PROTECTION

Trade secrets are a vital form of intellectual property that protects confidential business information and provides enterprises with a competitive advantage. As innovation and knowledge-based industries continue to expand, effective protection of trade secrets has become increasingly important. However, approaches to trade secret protection differ across jurisdictions, with some countries relying on dedicated legislation and others on common law, contractual obligations, unfair competition principles, or a combination of these mechanisms.

Disclosure, 2016 O.J. (L 157) 1; Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1839.

[4] Agreement on Trade-Related Aspects of Intellectual Property Rights, April l5, 1994, Marrakesh-Agreement Establishing the World Trade organization, Annex 1c. 1869 U.N.T.S. 299,33 I.L.M. I197 (1994) [hereinafter, "TRlPS"].

[5] Markus Peter and Martin Michaelis, "section 7: Protection of Undisclosed Information" in Peter-Tobias Stoll, Jan Busche *et.al*. (eds.), *WTO- Trade-Related Aspects of Intellectual Property* Rights 637 (Martinus Nijhoff Publishers, 2009).

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Volume 13 Issue 06 June 2026

This section provides a comparative overview of the legal frameworks governing trade secret protection in the United States, the United Kingdom, the European Union, and India, highlighting their key features, enforcement mechanisms, and approaches towards safeguarding confidential business information.

A. United States of America

Protection of trade secrets in the United States of America is broadly covered under the following legislations:

a. Uniform Trade Secrets Act of 1985

The UTSA defines a trade secret as any information, including a formula, pattern, compilation, program, device, method, technique, or process, that (a) derives actual or potential independent economic value from not being generally known to, or readily ascertainable by proper means by, persons who could obtain economic value from its disclosure or use, and (b) is subject to reasonable efforts, under the circumstances, to maintain its secrecy. The Act further defines "misappropriation" as the acquisition, disclosure, or use of another person's trade secret without express or implied consent by an individual who has acquired the information through improper means or who knew, or had reason to know, that the trade secret had been obtained through improper means. The term "improper means" includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, and espionage conducted through electronic or other means.

b. Economic Espionage Act of 1996

The Economic Espionage Act (EEA) is another important federal statute that deals with trade secret misappropriation and economic espionage. The Act adopts a definition of "trade secret" that is consistent with the definition provided under the Uniform Trade Secrets Act (UTSA)[6]. Under the EEA, an offence of trade secret theft is committed when an individual or organization knowingly misappropriates a trade secret related to a product involved in interstate or foreign commerce, with the understanding that such misappropriation will harm the owner of the trade secret while benefiting another person or entity.

Individuals found guilty of trade secret theft may be punished with imprisonment for up to ten years and/or a fine of up to $250,000 or twice the amount of the gain or loss resulting from the offence. Organizations, on the other hand, may be subject to fines of up to $5 million, twice the amount of the gain or loss associated with the offence, or three times the value of the stolen trade secret[7].

B. Defend Trade Secrets Act of 2016

The Defend Trade Secrets Act (DTSA), 2016, enacted in May 2016, is the latest U.S. legislation on trade secret protection and enables trade secret owners to bring civil actions for misappropriation before federal courts. The Act establishes federal jurisdiction in addition to state-level protection under the UTSA and adopts similar definitions of "trade secret," "misappropriation," and "improper means." It also grants whistleblower immunity to employees who confidentially disclose trade secrets to government authorities or attorneys for the purpose of reporting or investigating suspected legal violations.

Further, the DTSA provides remedies such as injunctions, damages for actual loss or unjust enrichment, exemplary damages of up to twice the compensatory amount in cases of willful or malicious misappropriation, and attorney's fees to the prevailing party in cases involving bad faith or malicious conduct. The Act also authorizes ex-parte seizure orders, subject to strict procedural requirements, to prevent the dissemination of trade secrets and strengthens criminal penalties for trade secret theft[8].

C. The European Union

The Council of the European Union adopted the Directive on the Protection of Undisclosed Know-how and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure to protect EU companies from trade secret theft[9]. Member States were given a maximum period of two years from the publication of the Directive in the Official Journal of the European Union to incorporate its provisions into their domestic legal systems. The Directive was adopted with the objective of addressing disparities in trade secret protection among Member States and ensuring a uniform level of protection for trade secrets across the European Union.

The key features of the Directive are as follows[10]:

i. It establishes a uniform definition of "trade secrets" covering valuable know-how, business information, and technological information where there is a legitimate interest in maintaining confidentiality and a reasonable expectation that such confidentiality will be preserved. The definition largely reflects the standards contained in the UTSA and Article 39 of the TRIPS Agreement.
ii. The Directive seeks to harmonize trade secret protection across the European Union and provides civil remedies against the unlawful acquisition, use, or disclosure of trade secrets. It also recognizes independent discovery and reverse engineering of a lawfully acquired product as lawful means of obtaining information, unless otherwise restricted by contract.

[6] 18 USC §1839; H- Rept 114-529 as amended by the DTSA.
[7] 18 USC §1831 (a), 3571 (d).
[8] 18 USC § 1836 (b) 2(A) (i).
[9] Council of the European Union, *Trade Secrets Protection: Council Adopts New Directive* (May 27, 2016), https://www.consilium.europa.eu/en/press/press-releases/2016/05/27-trade-secrets-new-directive/.
[10] Directive of the European Parliament and of the Council on the Protection of Undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, available at http://data.consilium.europa.eu/doc/document/PE-76-2015-INIT/en/pdf.

ISSN (Online) 2456 -1304
International Journal of Science, Engineering and Management (IJSEM)
Volume 13 Issue 06 June 2026

iii. The Directive incorporates whistleblower protections, permitting the disclosure of trade secrets where such disclosure is made in the public interest to expose misconduct, wrongdoing, or illegal activities. It also safeguards trade secrets disclosed during legal proceedings for their protection or defence.
iv. The remedies available under the Directive include compensation and damages for losses suffered by the trade secret holder, prohibition of the use or disclosure of trade secrets, restrictions on the manufacture, marketing, import, or export of infringing goods, destruction or surrender of materials containing trade secrets, and, where appropriate, publication of judicial decisions to deter future infringements.

Although Brexit requires continued observation of the United Kingdom's alignment with the standards established under the Directive, its immediate impact on trade secret law has been limited, as existing legal principles and protections continue to remain in force[11].

D. United Kingdom

In the United Kingdom, whether trade secrets constitute a form of "property" remains uncertain, and the prevailing view is that they do not fall within the traditional concept of property. Nevertheless, trade secrets are protected through various legal mechanisms, including breach of contract claims based on express or implied non-disclosure agreements, other confidentiality obligations, common law actions for breach of confidence, and statutory protections[12].

A common law action for breach of confidence is founded on the principle that information received in confidence must not be used unfairly or in a manner that harms the person who disclosed it. This principle is recognized in both England and Scotland. To qualify for protection, the information must possess the necessary quality of confidence and must be disclosed in circumstances creating an obligation of confidence, whether arising from a contract, the nature of the disclosure, or relationships such as that between employer and employee. However, particularly in employment relationships, post-termination protection is limited unless the information possesses a high degree of confidentiality, with highly sensitive trade secrets potentially receiving indefinite protection[13].

Trade secrets and confidential information are protected under common law and equity, while Scottish law relies on common law principles rather than equity. The Trade Secrets (Enforcement, etc.) Regulations 2018 further strengthened protection by defining a trade secret as information that is secret, has commercial value because of its secrecy, and is subject to reasonable steps to maintain confidentiality[14].

The Regulations prohibit the unauthorized acquisition, use, or disclosure of trade secrets, including unauthorized access[15]. Since infringement may arise from any one of these acts, a trade secret may be infringed even where it was lawfully acquired but subsequently used or disclosed unlawfully. Remedies include damages aimed at compensating losses, generally limited to the royalties or fees that would have been payable under a licence agreement[16].

UK courts also employ various measures to preserve confidentiality during litigation, including closed hearings, confidentiality orders, restricted access to evidence through confidentiality clubs, and redaction of judgments[17]. The Regulations further require trade secrets to remain confidential both during and after legal proceedings and prohibit participants in such proceedings from using or disclosing the protected information[18].

E. INDIA

At present, India does not have a dedicated statute governing the protection of trade secrets and confidential information. Such information is primarily protected through contractual obligations, equitable principles, and the common law action for breach of confidence. In the absence of a contractual arrangement, parties must rely on the tort of breach of confidence to safeguard trade secrets.

Although Section 27 of the Indian Contract Act, 1872 renders agreements in restraint of trade void, Indian courts have recognized reasonable restrictions aimed at protecting confidential information. In *Niranjan Shankar Golikari v. Century Spinning & Manufacturing Co. Ltd.*, the Supreme Court upheld reasonable restrictive covenants in employment contracts[19]. Similarly, in *VFS Global Services Pvt. Ltd. v. Mr. Suprit Roy*[20], the Bombay High Court held that restrictions on the use of trade secrets during or after employment do not

[11] Daniel Corbett & Ors, 'Brexit's Potential Impact For Trade Secrets in the UK', available at http://blogs.orrick.com/trade-secrets-watch/2016/07/14/brexits-potential-impact-for-trade-secrets-inthe-uk/.
[12] DLA piper, -"DLA Piper's Guide to Going Global - Intellectual Property and Technology- United Kingdom" 9 (February 9, 2023), available at: file:///C:/Users/UNDER%20SECRETARY/Downloads/DLA-Piper-Guide-toOoing-Clobal-lPT-United-Kingdom.pdf (last visited on June 01, 2026).
[13] Tom Scourfield, Joel Vertes. "Trade Secret Laws and Regulations in the UK CMS Law", (2022) available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-trade-secrets/united-kingdom (last visited on June 01, 2026).
[14] Scottish Law Commission No. 90, Breach of Confidence 5 (1984)' available at: https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scotlawcom.gov.uk /files/5712/8015/1448/26-07- 2010_1437_886.pdf (last visited on June 01, 2026).
[15] Tanya Aplin and Richard Arnold, "UK Implementation of the Trade Secrets Directive" J. Schavasha, T. Minssen and T. Riis (Eds). The Harmonisation and Protection of Trade Secrets in the EU. An appraisal of the EU Directive 65-85 (2020), available at: http://dx.doi.org/10.2139/ssrn.3393593 (last visited on June 01, 2026).
[16] The Trade Secrets (Enforcement, Etc.) Regulations 20l8 (2018 No.597), s. l6(2).
[17] Herbert Smith Freehills, *UK: Definition and Protection of Trade Secrets and Undisclosed Know-How to Be Harmonised Across Europe* (Jan. 10, 2014), https://hsfnotes.com/employment/2014/01/10/uk-definition-and-protection-of-trade-secrets-and-undisclosed-know-how-to-be-harmonised-across-europe/(last visited on June 01, 2026).
[18] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (SI 2018/597), s. 10(1).
[19] Niranjan Shankar Golikari v Century Spinning & Manufacturing Co. Ltd., 1967 AIR 1098.
[20] VFS Global Services Pvt. Ltd. v Mr. Suprit Roy, 2008 (2) BomCR 446.

amount to a restraint of trade under Section 27 and may be enforceable under appropriate circumstances. Consequently, contractual obligations remain a significant means of protecting trade secrets in India.

In *American Express Bank Ltd. v. Priya Puri*[21], the Delhi High Court defined trade secrets as formulas, technical know-how, or unique business methods unknown to others, excluding routine business information commonly known within the industry. Drawing from English common law principles, Indian courts have recognized three essential requirements for an action for breach of confidence[22]:

(i) the information must possess the necessary quality of confidence;
(ii) it must be communicated in circumstances imposing an obligation of confidence; and
(iii) there must be unauthorized use of the information causing detriment to the party disclosing it.

Further, in *John Richard Brady v. Chemical Process Equipments Pvt. Ltd*[23]., the Delhi High Court identified situations giving rise to breach of confidence claims, including unauthorized disclosure by employees, inducement by third parties to obtain confidential information, and breach of confidentiality obligations under know-how licensing arrangements.

The remedies available for breach of confidence include injunctions restraining disclosure, return of confidential information, compensation or damages based on the value of the confidential information, and delivery of infringing materials. Criminal liability may also arise under Section 72 of the Information Technology Act, 2000 for the unauthorized disclosure of electronic information, and under Sections 316 and 318 of the Bharatiya Nyaya Sanhita, 2023, which deal with criminal breach of trust and cheating respectively, subject to judicial determination of whether trade secrets constitute "property" for the purposes of these provisions.

IV. COMPARATIVE ANALYSIS: STRENGTHS AND WEAKNESSES

A comparative analysis of the trade secret protection frameworks in the United States, the European Union, the United Kingdom, and India reveals significant differences in their legal approaches, enforcement mechanisms, and remedial frameworks. While the United States and the European Union have adopted comprehensive statutory regimes, the United Kingdom and India continue to rely substantially on common law principles and contractual obligations.

Strengths:

United States: The United States has one of the most comprehensive trade secret protection regimes. The combined operation of the Uniform Trade Secrets Act (UTSA), the Economic Espionage Act (EEA), and the Defend Trade Secrets Act (DTSA) provides a clear legal framework at both state and federal levels. The DTSA offers federal jurisdiction, whistleblower protection, ex-parte seizure remedies, enhanced civil remedies, and criminal sanctions, ensuring robust protection and enforcement of trade secret rights.

European Union: The EU Trade Secrets Directive establishes a harmonized framework for trade secret protection across Member States. It provides a uniform definition of trade secrets, recognizes lawful means of acquisition such as independent discovery and reverse engineering, incorporates whistleblower protections, and offers comprehensive civil remedies. The Directive enhances legal certainty and consistency throughout the European Union.

United Kingdom: The United Kingdom benefits from a well-developed common law system based on the doctrine of breach of confidence, supplemented by the Trade Secrets (Enforcement, etc.) Regulations 2018. The framework provides flexibility in addressing diverse factual situations while ensuring statutory protection against unauthorized acquisition, use, or disclosure of trade secrets. UK courts also employ effective procedural safeguards to maintain confidentiality during litigation.

India: India's trade secret protection regime is supported by established principles of breach of confidence, contractual obligations, and judicial precedents. Courts have recognized and enforced confidentiality obligations in employment relationships and commercial transactions. The availability of equitable remedies such as injunctions and damages provides a degree of protection for confidential business information.

Weaknesses:

United States: Despite its comprehensive framework, the coexistence of federal and state laws may occasionally create procedural complexities. The broad scope of the statutory definition of trade secrets also requires careful judicial interpretation to avoid overprotection.

European Union: Although the Directive seeks harmonization, variations in implementation and judicial interpretation among Member States may affect uniform enforcement. The effectiveness of protection therefore depends on the domestic legal systems of individual Member States.

United Kingdom: The continued reliance on common law principles may result in less predictability compared to jurisdictions with dedicated trade secret statutes. The determination of confidential information often depends on factual circumstances, which may lead to uncertainty in enforcement.

[21] American Express Bank v. Priya Puri, (2006) IIILLJ 540 Del.
[22] *Emergent Genetics India Pvt. Ltd. v. Shailendra Shivam*, 2011 (125) DLT 173 (Del. HC) (India).
[23] John Richard Brady & Others v Chemical Process Equipment Pvt. Ltd., Delhi High Court, AIR 1987 Delhi 372.

India: The absence of a dedicated trade secrets legislation remains the most significant weakness of the Indian framework. Protection is fragmented across contract law, equity, common law principles, and limited statutory provisions. The lack of a codified definition of trade secrets, inconsistent enforcement standards, and limited remedies create uncertainty for businesses. Additionally, the existing framework may not adequately address modern challenges such as cyber theft, corporate espionage, and cross-border misappropriation of confidential information.

V. BEST PRACTICES AND RECOMMENDATIONS FOR EFFECTIVE TRADE SECRET PROTECTION

Irrespective of the legal framework adopted by a jurisdiction, the effective protection of trade secrets depends largely on the implementation of robust organizational, contractual, and technological safeguards. A review of practices followed in the United States, the United Kingdom, and the European Union highlights several measures that may be particularly beneficial for businesses operating in India.

1. Identification and Classification of Trade Secrets: Organizations should systematically identify, classify, and document information that qualifies as a trade secret. Periodic audits should be conducted to map valuable confidential information across business functions, ensuring that sensitive data is clearly designated and appropriately protected.

2. Adoption of Reasonable Security Measures: Since legal protection often depends on demonstrating reasonable efforts to maintain secrecy, businesses should implement comprehensive security measures, including:

- Physical security controls such as restricted access areas, secure storage systems, and visitor management protocols;
- Cybersecurity measures, including encryption, multi-factor authentication, firewalls, access monitoring, and data loss prevention systems; and
- Document management policies regulating access, retention, and secure disposal of confidential information.

3. Strengthening Contractual Protection: Well-drafted Non-Disclosure Agreements (NDAs), confidentiality clauses, and intellectual property protection provisions should be incorporated into employment contracts, consultancy agreements, vendor arrangements, and business partnerships. Such agreements should clearly define confidential information, obligations of the parties, and consequences of breach.

4. Employee Awareness and Compliance Programs: Regular training programs should be conducted to educate employees about trade secret protection, confidentiality obligations, cyber risks, and corporate policies. Creating a culture of confidentiality significantly reduces the risk of inadvertent disclosure.

5. Access Control and Information Governance: Access to trade secrets should be granted strictly on a "need-to-know" basis. Organizations should implement role-based access controls, maintain access logs, and periodically review authorization levels to minimise unauthorised exposure of sensitive information.

6. Monitoring and Risk Assessment: Continuous monitoring of access to confidential information and periodic security audits can assist in identifying vulnerabilities, detecting potential breaches, and ensuring compliance with internal protection measures.

7. Post-Employment Protection Measures: Exit interviews should be conducted with departing employees to reinforce confidentiality obligations and ensure the return of all proprietary information. Where legally permissible, reasonable non-solicitation and confidentiality obligations may further safeguard trade secrets after termination of employment.

8. Incident Response and Enforcement Strategy: Businesses should establish a dedicated incident response mechanism for addressing suspected trade secret misappropriation. Such a framework should include procedures for investigation, evidence preservation, containment of disclosures, regulatory reporting where necessary, and prompt legal action.

9. Enactment of a Dedicated Trade Secrets Legislation in India: Drawing lessons from the DTSA in the United States and the EU Trade Secrets Directive, India should consider enacting a comprehensive, standalone statute governing trade secret protection. Such legislation should provide a clear definition of trade secrets, establish uniform standards for enforcement, prescribe civil and criminal remedies, and address modern challenges such as cyber theft, corporate espionage, and cross-border misappropriation.

10. Promotion of Corporate Governance and Compliance Frameworks: Indian enterprises should integrate trade secret management into their corporate governance structures by adopting internal compliance policies, risk management frameworks, and board-level oversight mechanisms. This would strengthen business confidence, encourage innovation, and align Indian practices with international standards.

REFERENCES

[1] Benjamin Franklin, *Poor Richard's Almanack* (1735).
[2] David S. Almeling et al., A Statistical Analysis of Trade Secret Litigation in Federal Courts, 45 Gonz. L. Rev. 291, 292–95 (2010).
[3] 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, 2016 O.J. (L 157) 1; Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1839.
[4] Agreement on Trade-Related Aspects of Intellectual Property Rights, April l5, 1994, Marrakesh-Agreement Establishing the World Trade organization, Annex 1c. 1869 U.N.T.S. 299,33 I.L.M. I197 (1994) [hereinafter, "TRlPS"].
[5] Markus Peter and Martin Michaelis, "section 7: Protection of Undisclosed Information" in Peter-Tobias Stoll, Jan Busche *et.al*. (eds.), *WTO- Trade-Related Aspects of Intellectual Property* Rights 637 (Martinus Nijhoff Publishers, 2009).
[6] 18 USC §1839; H- Rept 114-529 as amended by the DTSA.

[7] 18 USC §1831 (a), 3571 (d).
[8] 18 USC § 1836 (b) 2(A) (i).
[9] Council of the European Union, *Trade Secrets Protection: Council Adopts New Directive* (May 27, 2016), https://www.consilium.europa.eu/en/press/press-releases/2016/05/27-trade-secrets-new-directive/.
[10] Directive of the European Parliament and of the Council on the Protection of Undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, available at http://data.consilium.europa.eu/doc/document/PE-76-2015-INIT/en/pdf.
[11] Daniel Corbett & Ors, 'Brexit's Potential Impact For Trade Secrets in the UK', available at http://blogs.orrick.com/trade-secrets-watch/2016/07/14/brexits-potential-impact-for-trade-secrets-inthe-uk/.
[12] DLA piper, -"DLA Piper's Guide to Going Global - Intellectual Property and Technology- United Kingdom" 9 (February 9, 2023), available at: file:///C:/Users/UNDER%20SECRETARY/Downloads/DLA-Piper-Guide-toOoing-Clobal-lPT-United-Kingdom.pdf (last visited on June 01, 2026).
[13] Tom Scourfield, Joel Vertes. "Trade Secret Laws and Regulations in the UK CMS Law", (2022) available at: https://cms.law/en/int/expert-guides/cms-expert-guide-to-trade-secrets/united-kingdom (last visited on June 01, 2026).
[14] Scottish Law Commission No. 90, Breach of Confidence 5 (1984)' available at: https://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scotlawcom.gov.uk/files/5712/8015/1448/26-07-2010_1437_886.pdf (last visited on June 01, 2026).
[15] Tanya Aplin and Richard Arnold, "UK Implementation of the Trade Secrets Directive" J. Schavasha, T. Minssen and T. Riis (Eds). The Harmonisation and Protection of Trade Secrets in the EU. An appraisal of the EU Directive 65-85 (2020), available at: http://dx.doi.org/10.2139/ssrn.3393593 (last visited on June 01, 2026).
[16] The Trade Secrets (Enforcement, Etc.) Regulations 20l8 (2018 No.597), s. l6(2).
[17] Herbert Smith Freehills, *UK: Definition and Protection of Trade Secrets and Undisclosed Know-How to Be Harmonised Across Europe* (Jan. 10, 2014), https://hsfnotes.com/employment/2014/01/10/uk-definition-and-protection-of-trade-secrets-and-undisclosed-know-how-to-be-harmonised-across-europe/(last visited on June 01, 2026).
[18] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (SI 2018/597), s. 10(1).
[19] Niranjan Shankar Golikari v Century Spinning & Manufacturing Co. Ltd., 1967 AIR 1098.
[20] VFS Global Services Pvt. Ltd. v Mr. Suprit Roy, 2008 (2) BomCR 446.
[21] American Express Bank v. Priya Puri, (2006) IIILLJ 540 Del.
[22] *Emergent Genetics India Pvt. Ltd. v. Shailendra Shivam*, 2011 (125) DLT 173 (Del. HC) (India).
[23] John Richard Brady & Others v Chemical Process Equipment Pvt. Ltd., Delhi High Court, AIR 1987 Delhi 372.