



RESEARCH ARTICLE



The Economic Impact of Trade Secret Misappropriation in The United States

Zammy A. Owodunni

LL. B, B.L., LL.M, Louisiana State University

*Corresponding: owodunnizammy@gmail.com

Received: 23.06.2026

Accepted: 13.08.2026

Publication date: 31.08.2026

ABSTRACT

In this paper, I analyze the economic impact of trade secret misappropriation in the United States. This is done by looking at the legal framework, the practical mechanics and typology of misappropriation, plus how harm ends up spreading across sectors, and then the direct microeconomic and broader macroeconomic consequences. I start from the view that trade secrets have really become the most commercially weighty category of intellectual property for innovation-intensive firms in the United States. Still, they are also the most structurally fragile because legal protection basically hangs on secrecy, and any commercial activity tends to compromise that secrecy. Using recent empirical data, insider threat analyses, and federal case law under the Defend Trade Secrets Act of 2016, I argue that trade secret theft drains the U.S. economy somewhere between \$180 billion and \$540 billion every year. At the same time, this kind of misappropriation makes affected firms see revenue and research reductions of roughly 40 per cent within five years, and it also feeds into the annual loss of more than two million jobs. I then map out four main modes of misappropriation, i.e., insider acquisition, cyber intrusion, breaches of confidential relationships, and state-sponsored economic espionage. I also examine how these modes behave economically across technology, pharmaceutical, manufacturing, and financial services sectors. Finally, I conclude that the present legal framework tends to systematically underprice misappropriation when you compare it to its real social cost. On that basis, I propose targeted reforms. These reforms include recalibrating the damages regime, boosting enforcement capacity for small enterprises, and dealing with state-sponsored misappropriation through executive branch tools, which is kind of the missing lever.

Keywords: Trade secrets; intellectual property; Defend Trade Secrets Act; economic espionage; research and development investment; innovation.



This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).

1. Introduction

The contemporary knowledge-based economy stands on a contradiction. The competitive advantage enjoyed by firms operating in the most productive sectors of the US economy lies in information that would be value deprived when exposed to the public domain.¹ Unlike patents, which allow a firm to enjoy a monopoly because the technology is disclosed, or copyright, which protects the expression of ideas, the legal protection offered by trade secrets exists in information where the economic value of the information is dependent on keeping it a secret. The dependency on secrecy makes this form of intellectual property both highly valuable and highly vulnerable legally. A trade secret loses its value once the information is revealed in public, the circumstances of the disclosure regardless².

The United States' legal system has been faced with this dilemma for more than a century. It started with the recognition of trade secrets in *Peabody v. Norfolk* by the Massachusetts Supreme Court in 1868³. Continued with the creation of common law provisions, Restatement First of Torts in 1939 and Uniform Trade Secrets Act in 1979⁴. Ultimately, the federal government criminalized the act of trade secret theft with the Economic Espionage Act in 1996 and provided a federal civil cause of action for such act in the Defend Trade Secrets Act of 2016⁵. Every step of the legislative process was driven by the understanding of inadequacy of existing legal tools to combat the problem that US companies were facing.

This paper seeks to investigate if the current legal system is adequate to safeguard the economic interests of firms in the United States and the greater good of innovating. The characteristics of trade secret misappropriation are the major reasons that make enforcement difficult. The analysis developed across the following sections demonstrates that the Defend Trade Secrets Act and its state analogues represent genuine progress but fall structurally short in three respects. First, the expected liability imposed on rational mis appropriators is a small fraction of the true social cost of the theft. Second, their enforcement mechanisms remain practically inaccessible to the small and medium enterprises that bear a disproportionate share of the harm. Third, they are structurally incapable of addressing state-sponsored economic espionage because the principal actors operate beyond the reach of domestic legal processes.

This paper first establishes the conceptual and legal framework of trade secret protection, tracing the development of United States law and identifying its fundamental economic paradox. Then it examines the

¹ Christopher Buccafusco, Jonathan S Masur and Deepa Varadarajan, Trade Secrecy Information Paradox (2025) 100 Notre Dame L Rev 925

² Suzana Nashkova, Defining Trade Secrets in the United States Past and Present Challenges A Way Forward (2023) 54 IIC 634

³ *Peabody v Norfolk* 98 Mass 452 (1868)

⁴ Nashkova (n 3) 636

⁵ Charles Doyle, Stealing Trade Secrets and Economic Espionage An Abridged Overview of the Economic Espionage Act (Congressional Research Service Report R42682 2024)

mechanisms and types of misappropriation, providing an explanation of the four key forms of illegal conduct. The section that follows offers a detailed analysis of the impact of misappropriation by industry, considering the industries of technology, pharmaceuticals, manufacturing, and financial services that constitute the overwhelming share of cases of trade secret theft litigated federally. Afterward, it explores the microeconomic effects on the affected U.S. firms through an empirical discussion of the economic impact of misappropriation on revenues and research expenditures. Then assess the macroeconomic ramifications of misappropriation, which include the effects on GDP, innovation, and employment. Finally, it sets out policy recommendations to help re-tune the damage system, improve the position of small businesses, and confront state-sponsored espionage.

2. Conceptual Framework and Legal Landscape

The category of trade secrets holds a peculiar place in the system of intellectual property of the USA. In modern knowledge-based economy, such assets became very important for businesses and may even surpass the value of patents and trademarks.⁶ The assets of this type are kept confidential and do not enjoy any protection similar to the one that copyrights and patents receive. Economic value of such assets lies completely in their confidentiality.⁷ The assets include various sensitive data, such as designs, methods, formulas, customer lists, and marketing information. As opposed to copyright and patent law, where basic concepts have unified definitions regulated by international conventions or national legislation, the trade secret law was never treated in the same way and remained mostly governed by common law up until recently. The economic significance of such an oversight is enormous: annual economic losses caused by theft of trade secrets have been estimated at over \$300 billion, which the US Senate called in 2016 as “comparable to the current level of U.S. exports to Asia.”⁸ Broader analyses suggest the true range may extend from \$180 billion to \$540 billion annually, representing between one and three per cent of gross domestic product.⁹

⁶ Janist Dhanol and Pradip Kumar Kashyap, A Comparative Analysis of Trade Secret Protection in the USA, UK, Australia, and India (2024) 30 Educational Administration: Theory and Practice 6654.

⁷ Ibid

⁸ US Senate, Report on the Defend Trade Secrets Act of 2016, S Rep No 114-220, 114th Cong, 2nd Sess (2016) 2.

⁹ Commission on the Theft of American Intellectual Property, *IP Commission Report: The Theft of American Intellectual Property* (National Bureau of Asian Research, Update 2017).

Figure 1. Key Legislative and Doctrinal Milestones in US Trade Secret Law



Figure 1. Key Legislative and Doctrinal Milestones in United States Trade Secret Law (1939-2023)

The concept was introduced into United States legal terminology in the nineteenth century to accommodate the protection of new assets emerging during the transition from agrarian to manufacturing production.¹⁰ Early judicial proceedings focused not on providing a precise definition but rather on conceptualising the meaning of a trade secret through description. The Supreme Court of Massachusetts in *Peabody v. Norfolk* established what appears to be the first dicta in this context, holding that trade secrets might relate to a relatively novel and safeguarded process of manufacture that gives its owner property rights worthy of court protection against unauthorized disclosure.¹¹ The first definitional pillar to achieve common law prominence was the Restatement First of Torts promulgated in 1939, which provided foundational principles for courts to interpret trade secret disputes.¹²

The absence of a unitary statutory regime meant that the subject matter and definitional parameters of trade secrets were shaped under the influence of various common law doctrines, which generated little certainty regarding their scope.¹³ Minor differences in the judicial perception of trade secrets created some disagreements between courts and thus paved the way for different rules to apply in the same area. Such an unclear situation made separate states seek a gradual orientation towards the implementation of statutes. In this regard, the first step was taken by the National Conference of Commissioners of Uniform State Laws, which provided a definition of a trade secret according to the Uniform Trade Secrets Act in 1979. It proposed a uniform law text for individual states to adopt and is currently implemented in 51 jurisdictions across the country.¹⁴

The federal government radically changed this situation after realizing the potential danger of corporate espionage. In 1996, Congress adopted the Economic Espionage Act in order to develop a federal statutory

¹⁰ibid 638.

¹¹ibid.

¹²ibid 637.

¹³ibid 635.

¹⁴ibid 638.

definition and criminalize the misappropriation of trade secrets where the appropriation of such property either aids a foreign entity or concerns interstate commerce. In addition to the above-mentioned criminal statute, the Defend Trade Secrets Act of 2016 was adopted later to amend the federal statutory definition and develop federal civil remedy. Thus, companies were able to bring misappropriators to court on the federal level without undermining the state laws. As a result, the current American trade secret protection system consists of state and federal statutes applied simultaneously, which gives rise to a multi-layered approach that provides criminal deterrence and monetary compensation for victims.

The impact of the legislative change in terms of its effect on the litigation process has been quite significant. In 2016, which was the year that saw the introduction of the DTSA, 173 cases had been filed in the United States district courts pursuant to the law. This number had increased to 600 by 2017, recording a 247% rise. 749 cases involving DTSA filings had been recorded in 2023, with total federal trade secret cases standing at 1,203 in 2023.¹⁵ As of 2024, United States district courts had received a cumulative total of 5,159 case filings involving DTSA claims since the Act's enactment.¹⁶

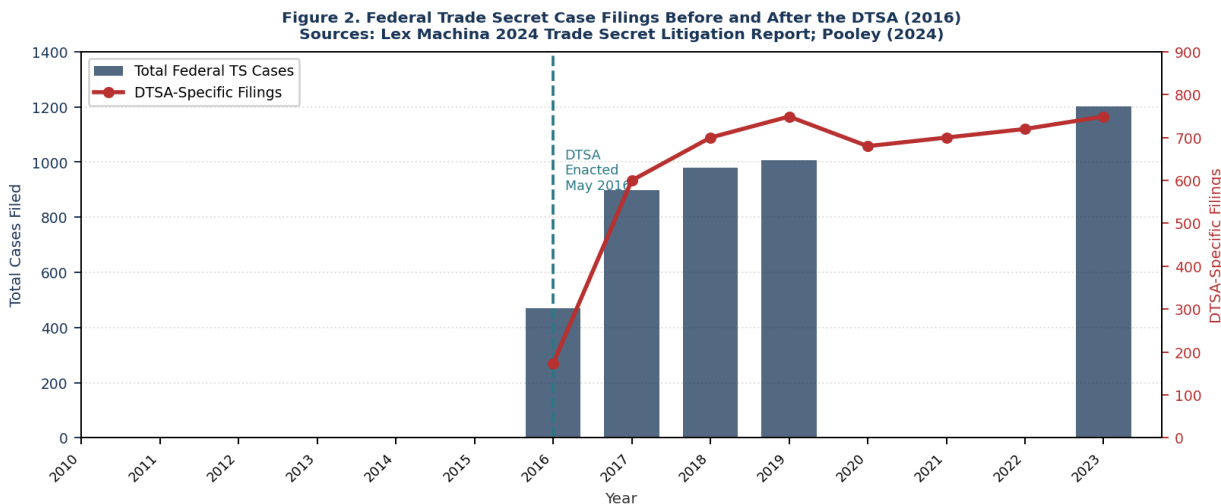


Figure 2. Federal Trade Secret Case Filings Before and After the Defend Trade Secrets Act (2016). Sources: Lex Machina 2024 Trade Secret Litigation Report; Pooley (2024)

There exists an economic paradox underlying the legal framework for trade secrets. The law fundamentally aims to encourage socially beneficial behaviors by allowing firms to protect their financial investments in the creation of valuable information.¹⁷ Protecting this information theoretically makes organisations more likely to fund research and development in the first instance. However, this same legal shield can be utilised

¹⁵ Lex Machina, 2024 Trade Secret Litigation Report (LexisNexis, 2024) 4; Carrier Management, “Report: Bump in Federal Trade Secret Litigation Seen in 2023” (17 September 2024).

¹⁶ James Pooley, “The US Defend Trade Secrets Act Eight Years On” IAM Trade Secrets Blog (14 May 2024).

¹⁷ Christopher Buccafusco, Jonathan S Masur and Deepa Varadarajan, *Trade Secrecy Information Paradox* (2025) 100 Notre Dame L Rev 925.

to conceal socially harmful behaviours or stifle market competition.¹⁸ Furthermore, trade secrets remain uniquely vulnerable compared to other forms of intellectual property. A patent retains its legal force even if an infringer illegally utilises the underlying invention. Conversely, a trade secret loses all legal protection the moment the information becomes public knowledge. This fragile nature necessitates continuous and costly security investments from companies, shifting the economic burden of protection heavily onto the private sector. The Office of the Director of National Intelligence has separately estimated that economic espionage conducted through cyber intrusion alone costs the United States economy \$400 billion per year, compounding the structural protection burden described above.¹⁹

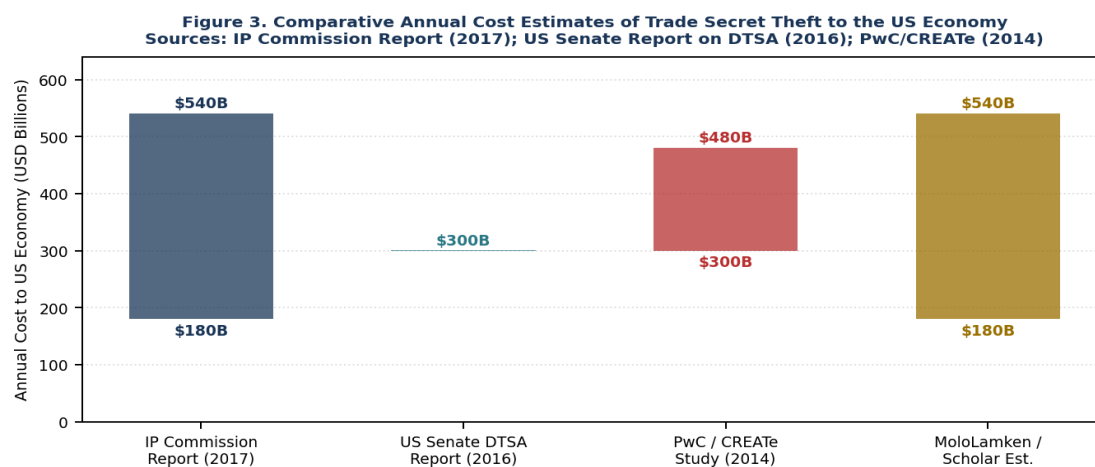


Figure 3. Comparative Annual Cost Estimates of Trade Secret Theft to the United States Economy Sources: IP Commission Report (2017); US Senate Report on the DTSA (2016); PwC/CREATE Study (2014)

It is important to understand the legal parameters around these matters, because it is vital for assessing the economic harm that can be suffered once the protective shield is sort of broken down. The empirical research that has been done on lawsuits indicates that the usual path where misappropriation shows up is not so much the work of foreign spies or hacker attacks, but more often insider treachery. It has been found that roughly 85 per cent of the federal trade secrets cases that were studied involved people who already had personal access to the trade secrets, through their position of trust within the organization.²⁰ Another detail corroborates this same idea is that, around 70 per cent of all trade secret cases also come with claims of breach of contract.²¹ Trade secret cases in federal courts doubled between 1988 and 1995, doubled again between 1995 and 2004, and doubled yet again by 2017, reflecting the growing economic stakes attached to

¹⁸ibid 926.

¹⁹Office of the Director of National Intelligence, *Foreign Economic Espionage in Cyberspace* (2018) 1; IP Commission Report (n 18) 1.

²⁰ David S Almeling and others, "A Statistical Analysis of Trade Secret Litigation in Federal Courts" (2010) 45 Gonzaga L Rev 291, 302-304.

²¹Walter Pfeffer and Harman Deol, "How to Protect Precious IP from Layoff-Related Insider Theft" (Corporate Compliance Insights, 7 June 2023); Almeling (n 26) 303.

proprietary information in the modern knowledge economy.²²

Figure 4. Identity of Misappropriators in Federal Trade Secret Cases
 Source: Almeling et al. (2010); Corporate Compliance Insights (2023)

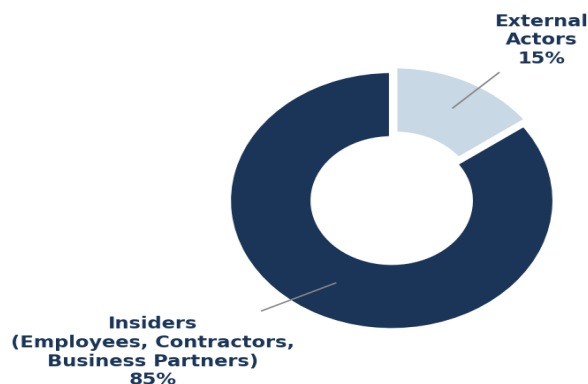


Figure 4. Identity of Misappropriators in Federal Trade Secret Cases Sources: Almeling et al. (2010); Corporate Compliance Insights (2023)

Table 1. The Public Policy Paradox of Trade Secret Law

Protective Function	Potential for Abuse or Market Harm
Incentivises investment in research and development by guaranteeing that commercially valuable discoveries can be shielded from competitors	May be deployed to conceal unsafe products, dangerous manufacturing processes, or anti-competitive practices from regulatory oversight and public scrutiny
Encourages the creation of specialised proprietary knowledge that generates competitive advantage and drives broader economic productivity	Allows dominant incumbents to suppress disclosure of information that could enable competitors to enter markets, potentially stifling rather than stimulating innovation
Provides perpetual protection that does not expire, rewarding sustained commitment to maintaining secrecy and security infrastructure	Perpetual duration means the economic burden of protection remains indefinite, concentrating compliance costs within the private sector

²²Almeling (n 26) 303.

Protective Function	Potential for Abuse or Market Harm
Complements patent and copyright systems by covering information categories that do not satisfy requirements for formal IP registration	The absence of a registration requirement and the breadth of the definition create uncertainty, generating litigation risk for legitimate competitors engaged in parallel development

Source: Buccafusco, Masur and Varadarajan, "Trade Secrecy Information Paradox" (2025) 100 Notre Dame L Rev 925, 925-926.

3. Mechanics and Typology of Trade Secret Misappropriation

Having discussed the legal and conceptual framework surrounding the protection of trade secrets in the US, we can now take an in-depth look into the mechanisms that contribute to the failure of this protection. Under the Uniform Trade Secrets Act and the Defend Trade Secrets Act of 2016, the term ‘misappropriation’ refers to three basic forms of illegal activity: the wrong acquisition of a trade secret, the unauthorized disclosure of a trade secret, and the unauthorized use of a trade secret.²³ These three mechanisms of misappropriation do not exist in a vacuum; in reality, one case of misappropriation entails all three types of misconduct. To assess the economic impact that misappropriation can have on the company, we should understand the exact mechanics of how each form of misappropriation works.

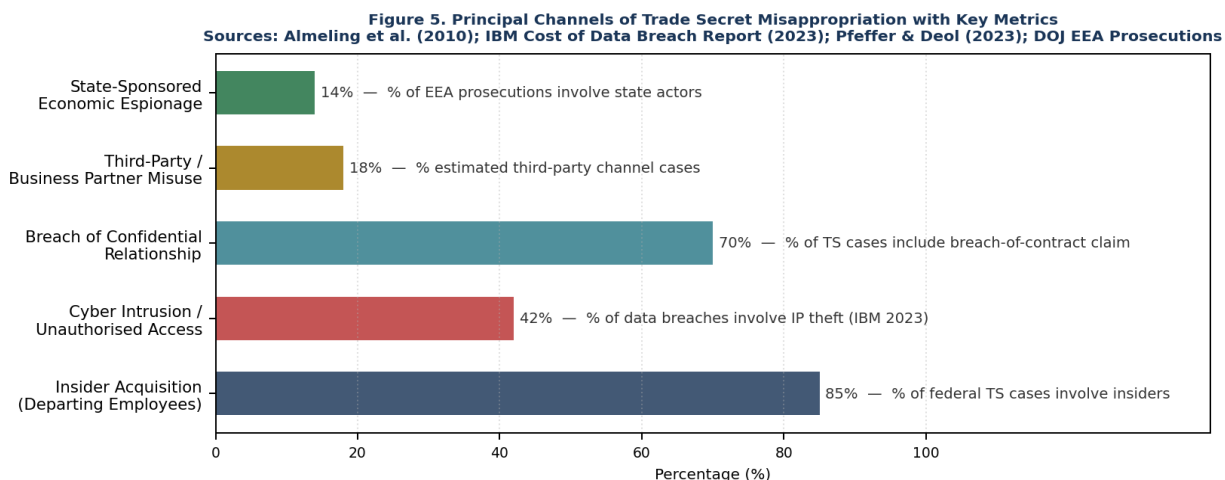


Figure 5. Principal Channels of Trade Secret Misappropriation with Key Metrics.

A. Insider Acquisition: The Departing Employee

The numerically dominant variety of trade secret misappropriation in the United States is insider acquisition,

²³ WIPO, Guide to Trade Secrets and Innovation, Part V (2024).

most often done by leaving employees who effectively move confidential information to a rival enterprise. Empirical analysis of federal trade secret cases seems to confirm that about 85 per cent of cases include individuals who already had legitimate, authorised access to the information they later misappropriated.²⁴ This percentage really shifts the whole story around trade secret theft, because the danger is not mainly some outside opponent trying to breach the perimeter of a locked system. Instead, it's an internal actor, taking advantage of the trust that authorised access tends to assume.

The typical mechanics of insider acquisition have been shaped by the digitalisation of the workplace. The departing employee who downloads confidential files to a personal device, uploads materials to a personal cloud account, or forwards company emails to a personal inbox in the final days of employment is now the most common factual scenario in trade secret litigation.²⁵ In *TF Global Markets Ltd v. Sorenson*, which was decided in 2023 by the Northern District of Illinois, the court essentially confirmed that when a former employee kept, without authorisation, a large number of confidential files, the plaintiff had alleged misappropriation well enough via "acquisition by improper means" to make it past a motion to dismiss.²⁶ And, the reach or magnitude of that kind of conduct feels bigger, also because digital information can be pulled out rather easily, without much friction.

The economic consequences of an insider acquisition are made worse by the time that is usually needed to notice the breach, or well, find it. Malicious insider incidents take an average of 142 days to detect, compared to 45 days for incidents caused by negligent employees.²⁷ In that detection window, the misappropriator may already have used the taken know-how to build competing products, approach the victim's customers, or obtain extra financing based on the misappropriated technology. And as the Ponemon Institute mentioned in its 2026 report, the average annual cost of insider-related incidents now sits at \$19.5 million per organisation, a 123 per cent increase since 2018.²⁸

B. Cyber Intrusion and Unauthorized Digital Access

The second main mode of misappropriation is cyber intrusion: basically, the unauthorised electronic entry into a company's information systems, in order to pull out trade secret material. The Economic Espionage Act makes it a crime not only when someone physically takes a trade secret but also when they, without

²⁴ Stout, 2024 Trends in Trade Secret Litigation Report (Stout 2024) 18 <https://ts25.org/wp-content/uploads/2025/02/2024-stout-trends-in-trade-secrets-litigation-report-volume-3.pdf> accessed 7 May 2026.

²⁵ Congressional Research Service, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, R42681 (29 October 2024) 4-5.

²⁶ *TF Global Markets Ltd v Sorenson*, 2023 US Dist Lexis 27983 at *11-12 (ND Ill, 17 February 2023).

²⁷ Ponemon Institute, 2026 Cost of Insider Threats: Global per cent Report (Proofpoint, 2026) 3.

²⁸ Tim Londergan, "The Invisible Epidemic: Unprosecuted Trade Secret Theft" Tangibly (19 November 2025); Ponemon (n 36) 1.

authorisation, copy, download, upload, or otherwise transmit protected information.²⁹ Ransomware attacks, compromised credentials, and phishing campaigns have basically become the main digital pathways for trade secret theft, pushing aside the older physical intrusion scenarios that were more common in earlier case law.

IBM's 2023 Cost of a Data Breach Report said the average cost of a data breach in the United States hit \$4.45 million, and 43 percent of those breaches involved some kind of intellectual property theft.³⁰ That number doesn't really show the whole picture, though, because it mostly reflects only the direct expenses. The knock-on damage is harder to put a price on, but it can be bigger cumulatively, like the weakening of competitive advantage, the speeding up of a rival's development schedule, and also the potential future licensing revenue that the misappropriated information might have helped generate.

The detection problem is especially acute when it comes to cyber intrusion. Unlike the departing employee who has to physically remove information in the days around termination, a successful cyber intruder can keep some form of persistent access to a target's systems for months or years. The average detection time for a cyber-intrusion that ends up with trade secret exfiltration is around 77 days, but more sophisticated state-sponsored intrusions may go unnoticed for a whole lot longer. This extended dwell time gives the intruder time for a systematic, almost comprehensive extraction of the most commercially valuable information the target has, while they tune and adjust the breadth of the theft so it does not accidentally trip the detection mechanisms.

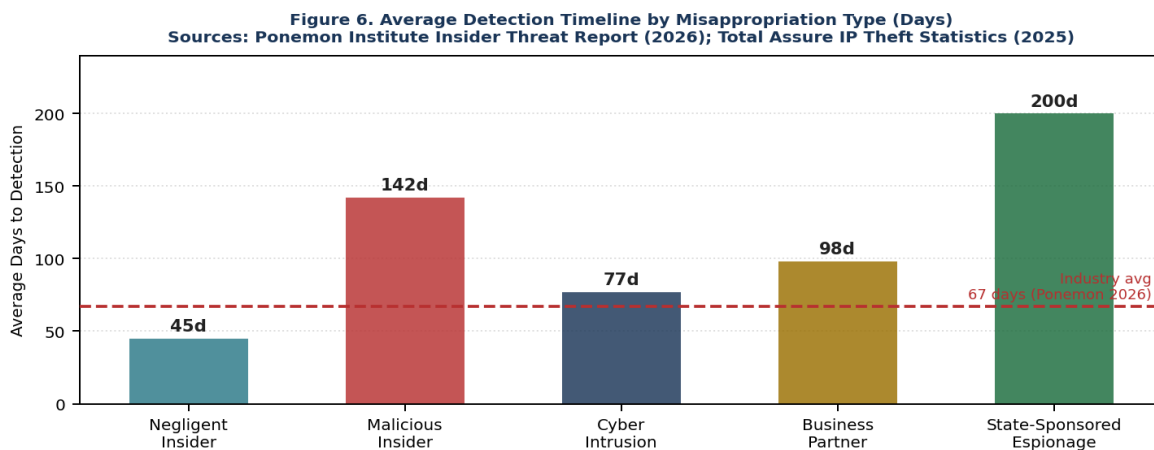


Figure 6. Average Detection Timeline by Misappropriation Type (Days). Sources: Ponemon Institute Insider Threat Report (2026); Total Assure IP Theft Statistics (2025)

C. Breach of Confidential Relationship and Third-Party Disclosure

A third significant mode of misappropriation arises from the breach of a confidential relationship that does

²⁹ CRS Report (n 31) 5-6; 18 USC s 1832(a)(2).

³⁰ IBM Security, Cost of a Data Breach Report 2023 (IBM, per cent2023) 1, 11.

not necessarily involve an employment context. Trade secrets are routinely disclosed to third parties in the course of legitimate commercial activity: to prospective investors in due diligence, to suppliers in manufacturing arrangements, to potential acquirers in merger negotiations, and to licensees under contractual arrangements.³¹ The breach of these obligations constitutes misappropriation regardless of whether the information is subsequently used commercially, because the DTSA definition of misappropriation encompasses unauthorised disclosure as a standalone category of wrongful conduct independent of actual use.

The practical importance of this subcategory of claims is highlighted by the 70 percent overlap of claims of breaches of contract in cases involving the misappropriation of trade secrets. This is due to the underlying reality that most business transactions involve a disclosure coupled with a non-disclosure agreement which results in a breach of contract and statutory misappropriation concurrently. The concomitant pleading of both categories of claims presents some strategic difficulties on the plaintiff's side as the identification of the particular trade secrets at stake becomes critical to avoid the trap of an "all or nothing" damages model, as demonstrated by the district court's ruling in *Versata Software, Inc v. Ford Motor Company* in 2023 when the damages expert failed to distinguish his analysis among the different trade secrets, leading to the reversal of the damages award of more than \$100 million.

D. State-Sponsored Economic Espionage

The most economically significant but least frequently prosecuted mode of misappropriation is state-sponsored economic espionage. This is the direct theft of United States trade secrets by foreign governments or their instrumentalities for the purpose of advancing the economic and technological competitiveness of the sponsoring state.³² The Economic Espionage Act addresses this category specifically under section 1831, which criminalizes trade secret theft where the intended beneficiary is a foreign government or one of its organs. Unlike section 1832, which requires proof that the defendant knew the misappropriation would injure the owner to the benefit of a third party, section 1831 requires only proof of intent to benefit a foreign government.

State-sponsored espionage represents the most technically sophisticated form of misappropriation and the most difficult to detect and attribute. Empirical analysis of Economic Espionage Act prosecutions has found that approximately 14 per cent involve state actors.³³ However, this figure significantly understates the true scale of state sponsored theft, mainly because the prosecution rate for offences that involve foreign

³¹WIPO (n 29); CRS Report (n 31) 6-7.

³²18 USC s 1831; CRS Report (n 31) 2-3.

³³Sarah Morningstar, "Trade Secret Theft Trends: A Closer Look at the Perpetrators" The Cipher Brief (5 June 2024); USTR, 2023 Special 301 Report (2023) 10-11.

governments is circumscribed by diplomatic, intelligence, and evidentiary constraints that do not show up to the same degree for domestic misappropriators. Current estimates from the National Counterintelligence and Security Center (NCSC) put the annual impact, of global intellectual property theft and cyber enabled espionage, somewhere between \$600 billion and \$1.2 trillion.³⁴ The People's Republic of China has been, over and over, identified by the Federal Bureau of Investigation and the Office of the United States Trade Representative as the principal wellspring of state supported trade secret theft, aimed at United States firms.

E. Economic Consequences and the Damages Framework

The economic consequences of trade secret misappropriation operate across multiple dimensions simultaneously. At the most immediate level, the victim suffers direct financial loss: the erosion of revenue that the trade secret would have generated had it remained exclusively under the victim's control, and the acceleration of a competitor's ability to enter a market or develop a competing product. At a secondary level, the victim bears substantial costs of litigation and investigation. Litigation costs for a trade secret case of any complexity routinely range from \$50,000 at the preliminary stage to \$1-5 million at trial, with high-stakes cases reaching \$25 million or more.³⁵

Judicial awards in trade secret cases have grown substantially in scale over the period since the enactment of the DTSA. In *Appian Corp v. Pegasystems Inc.*, a Virginia state jury awarded \$2 billion in 2022 following allegations of systematic corporate espionage.³⁶ In *TriZetto Group v. Syntel*, a Manhattan jury awarded \$855 million in 2020 for the misappropriation of a software platform.³⁷ In *Motorola Solutions v. Hytera Communications*, a jury awarded \$544 million for the systematic misappropriation of digital mobile radio technology.³⁸

³⁴ National Counterintelligence and Security Center, Foreign Economic Espionage in Cyberspace (ODNI 2018) 1 <https://www.dni.gov/files/NCSC/documents/news/20180724-ncsc-press-release-foreign-econ-esp-cyber.pdf> accessed 21 April 2026.

³⁵ American Intellectual Property Law Association, 2025 Report of the Economic Survey (AIPLA 2025) <<https://www.aipla.org/home/news-publications/economic-survey/2025-report-of-the-economic-survey>> accessed 20 May 2026.

³⁶ *Appian Corp v Pegasystems Inc*, Case No 1399-22-4 (Court of Appeals of Virginia, argued November 2023).

³⁷ *Syntel Sterling Best Shores Mauritius Ltd v The TriZetto Group Inc*, verdict October 2020 (SDNY); IPWatchdog, "2024 Trade Secret Update" (19 July 2024).

³⁸ *Motorola Solutions Inc v Hytera Communications Corp*, No 1:17-cv-01973 (ND Ill), jury verdict February 2020, reduced to \$544 million on appeal.

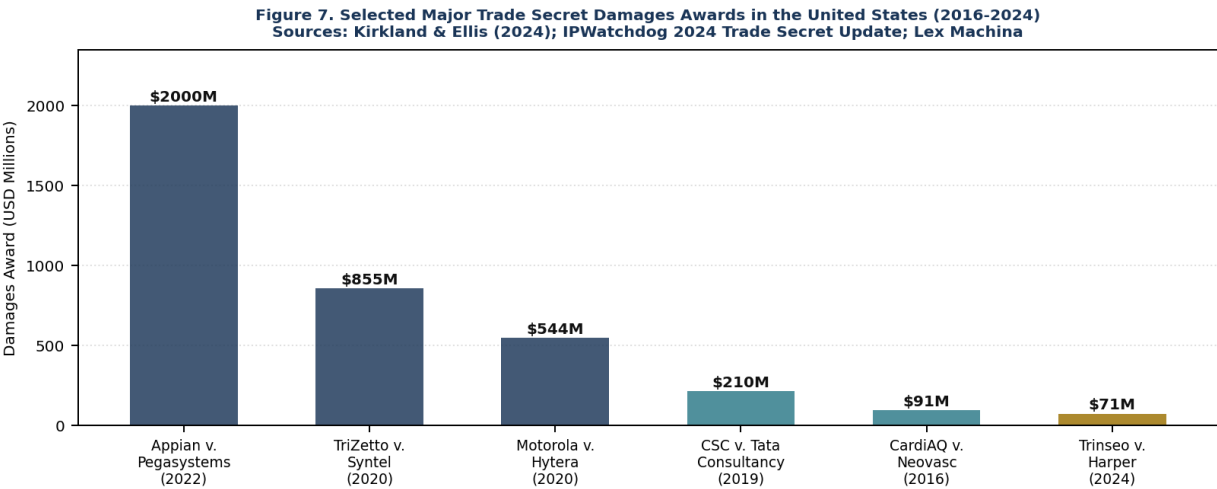


Figure 7. Selected Major Trade Secret Damages Awards in the United States (2016-2024) Sources: Kirkland & Ellis (2024); IPWatchdog 2024 Trade Secret Update; Lex Machina

Table 2. Summary Typology of Trade Secret Misappropriation in the United States

Mode	Primary Mechanism	Legal Basis (DTSA / EEA)	Key Economic Impact
Insider Acquisition (Departing Employee)	Downloading files, uploading to personal cloud, emailing confidential data before departure	18 USC s 1832; DTSA s 1836(b)(1); breach of NDA	85% of federal cases; avg \$19.5M/org annually (Ponemon 2026)
Cyber Intrusion (Unauthorised Access)	Hacking, phishing, ransomware, credential compromise, prolonged access	18 USC s 1832(a)(2); DTSA; CFAA 18 USC s 1030	43% of data breaches involve IP theft; the average breach cost \$4.45M (IBM 2023)
Breach of Confidential Relationship (Third-Party)	Misuse of disclosures in due diligence, licensing, supply chain, or joint venture	DTSA s 1836(b)(1); breach of NDA; UTSA misappropriation	70% of TS cases include breach-of-contract claim; litigation risk for all

Mode	Primary Mechanism	Legal Basis (DTSA / EEA)	Key Economic Impact
Disclosure)	contexts		commercial relationships
State-Sponsored Espionage (Economic Espionage)	Directed cyber intrusion, recruitment of insiders, bribery, and coercion by foreign governments	18 USC s 1831 (EEA); Foreign and Economic Espionage Penalty Enhancement Act 2012	Estimated \$400B/yr cyber espionage (ODNI 2018); 14% of EEA prosecutions involve state actors

Sources: Congressional Research Service (2024); Almeling et al. (2010); IBM (2023); Ponemon Institute (2026); ODNI (2018); DOJ EEA prosecution data.

The four modes of misappropriation documented in this section share a common structural feature: each exploits a necessary vulnerability in the commercial operation of firms that depend on trade secret protection.

4. Sectoral Analysis of Trade Secret Misappropriation

Arguably, the economic impact of trade secret misappropriation is not spread evenly across the United States economy. How bad it gets depends on whether a specific industry leans on proprietary technical and commercial information as its main competitive edge, and also how easily that kind of information can be passed along, duplicated, or decoded through reverse-engineering once it's been taken. As Figure 8 shows, the technology and software sector is responsible for roughly 38 per cent of federal trade secret litigation, then pharmaceuticals and life sciences at 21 per cent, manufacturing and industrial at 17 percent, and financial services at 12 per cent. When you zoom in on each sector you can see the shared structural weak spots as well as the particular features that shape what misappropriation really does economically in that area.

Figure 8. Distribution of Federal Trade Secret Litigation by Industry Sector
 Sources: Lex Machina 2024 Trade Secret Litigation Report; Almeling et al. (2010)

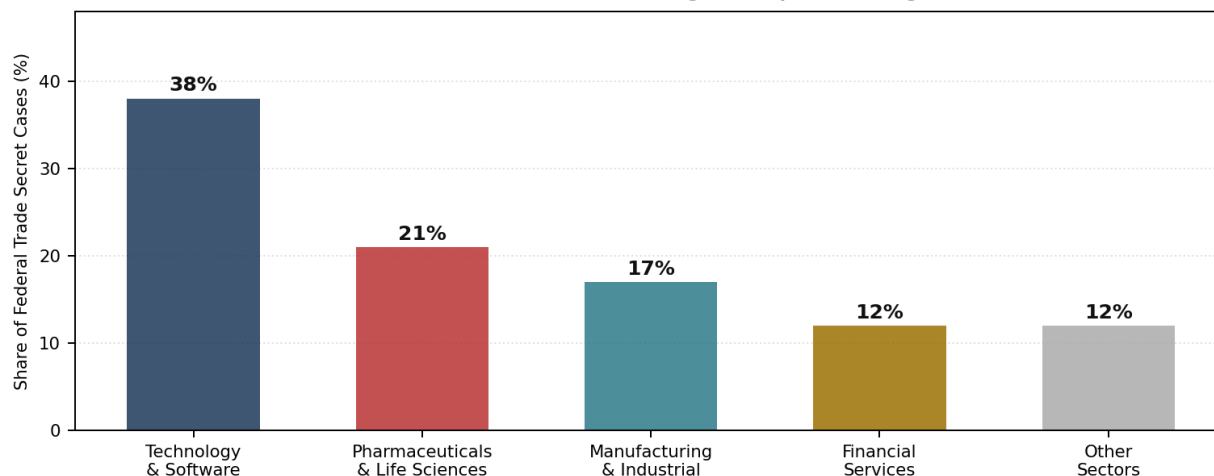


Figure 8. Distribution of Federal Trade Secret Litigation by Industry Sector Sources: Lex Machina 2024 Trade Secret Litigation Report; Almeling et al. (2010)

A. Technology and Software

The technology and software sector generates the largest volume of trade secret litigation in the United States by a substantial margin. This reflects both the concentration of commercially valuable proprietary information within the sector and the high employee mobility that characterises the technology labour market, particularly in jurisdictions such as California, where non-compete agreements are unenforceable. The sector's primary trade secrets encompass software source code and algorithms, product roadmaps and architecture designs, training data and machine learning model parameters, and customer acquisition and pricing data.³⁹

The cases that have defined trade secret liability in this sector illustrate the particular vulnerability of enterprise software firms, where the entire commercial value of a product may rest upon proprietary code that a single engineer can copy to a personal device in a matter of seconds. In *Appian Corp v. Pegasystems Inc*, the Virginia jury's \$2 billion verdict rested on findings that Pegasystems had engaged in a systematic campaign of corporate espionage by hiring a government contractor's employee who had legitimate access to Appian's platform to extract proprietary information about its architecture and functionality for use in product development.⁴⁰ In *Computer Sciences Corp v. Tata Consultancy Services Ltd*, a Texas federal jury awarded \$210 million after finding that Tata's employees had wilfully and maliciously misappropriated source code and documentation for life insurance administration software.⁴¹

³⁹WilmerHale, 2024 Trade Secret Update: A Look at Recent Trade Secret Developments and Trends (19 July 2024) 2-3.

⁴⁰Appian Corp v Pegasystems Inc (n 44); Kirkland and Ellis (n 43).

⁴¹Computer Sciences Corp v Tata Consultancy Services Ltd, No 3:15-CV-01187 (ND Tex), jury verdict November 2019.

The economic significance of technology sector trade secrets extends beyond the direct value of the stolen information to the structural incentives of the industry. A study by Ocean Tomo LLC estimated that intellectual property assets, including trade secrets, constitute more than 80 per cent of the market capitalisation of S&P 500 companies.⁴² In the technology sector, where valuations are driven predominantly by intangible assets, the misappropriation of core proprietary information does not merely reduce a company's competitive position; it can fundamentally undermine the economic rationale for the enterprise itself. The legal framework must therefore price misappropriation at a level that reflects not only the direct revenue loss but the destruction of enterprise value that a successful misappropriation implies.

B. Pharmaceuticals and Life Sciences

The pharmaceutical and life sciences sector presents a distinctive trade secret landscape shaped by the extraordinary cost and duration of research and development cycles. United States biopharmaceutical companies collectively spend approximately \$160 billion annually on R&D,⁴³ generating clinical trial data, manufacturing processes, formulation chemistry, and regulatory submissions that represent decades of scientific investment. Unlike the technology sector, where the competitive value of a trade secret may be exhausted relatively quickly by the pace of technological change, pharmaceutical trade secrets can retain their commercial significance for decades, because the manufacturing processes and formulation chemistry for complex biologics are inherently difficult to reverse-engineer.

The life sciences sector accounts for approximately 21 per cent of federal trade secret litigation,⁴⁴ with a disproportionate share of the most economically significant cases. In the life sciences sector, employee leaks are responsible for approximately 60 per cent of trade secret theft incidents, a figure consistent with the broader empirical pattern of insider dominance documented in the previous section.⁴⁵ The economic harm of pharmaceutical trade secret misappropriation is particularly severe because the stolen information typically represents an irreplaceable investment in scientific discovery. When a competitor obtains access to clinical trial data or manufacturing know-how through misappropriation, it eliminates years of R&D expenditure and regulatory compliance costs, which allows it to market competing products at prices that undercut the innovating firm's ability to recoup its investment.

⁴²Ocean Tomo LLC, *Annual Study of Intangible Asset Market Value* (2015) 1; ScienceDirect, "Trade secrets and cyber security breaches" (2022) 8 *Journal of Finance and Data Science* 202, 203.

⁴³US biopharmaceutical companies collectively spend approximately \$160 billion annually on R&D: *Frontiers in Bioengineering and Biotechnology* (2019) citing Research America (2016).

⁴⁴ Stout, 2024 Trends in Trade Secret Litigation Report (Stout 2024) 14 <<https://ts25.org/wp-content/uploads/2025/02/2024-stout-trends-in-trade-secrets-litigation-report-volume-3.pdf>> accessed 7 May 2026.

⁴⁵International Bar Association Health and Life Sciences Committee, "Trade secrets: a strategic element in the life sciences and biotechnology industries" (2024); Economist Intelligence Unit, "Open secrets? Guarding value in the intangible economy" (9 June 2021).

Two cases from 2023 and 2024 illustrate the sector's particular vulnerability. In *Insulet Corp v. EOFlow Co Ltd*, the Federal Circuit found that the district court had erred in granting a preliminary injunction that halted EOFlow's communications with Medtronic about a potential acquisition. The case arose from allegations that former Insulet employees who joined EOFlow had used knowledge of Insulet's OmniPod technology to accelerate EOFlow's competing product development.⁴⁶ The economic stakes were magnified by Medtronic's reported acquisition interest, underscoring how misappropriated pharmaceutical technology can distort the merger and acquisition market by inflating the apparent value of a potential target.

C. Manufacturing and Industrial

As at early 2026, the manufacturing and industrial sector accounts for approximately 26 percent of federal trade secret litigation,⁴⁷ with cases concentrated in advanced manufacturing processes, materials science, precision engineering, and supply chain management systems. The sector's trade secrets are characterised by their embeddedness in physical production processes, which makes them particularly difficult to protect because the information is necessarily shared with manufacturing personnel, equipment operators, and supply chain partners.

The Third Circuit's 2022 decision in *PPG Industries v. Jiangsu Tie Mao Glass Co* provides a paradigmatic illustration of manufacturing sector misappropriation. PPG had invested heavily in developing a proprietary plastic material for airplane windows, designated Opticor, with applications in the automotive and aerospace industries. Jiangsu Tie Mao Glass, a Chinese competitor, hired a former PPG employee who had worked on Opticor and used the misappropriated technical information to develop a competing product, shortcutting years of materials science research.⁴⁸ The case resulted in a Third Circuit ruling clarifying the application of the "saved cost" damages theory in trade secret cases, holding that avoided development costs are a permissible measure of the defendant's unjust gain.

The manufacturing sector is particularly exposed to state-sponsored misappropriation. The United States Trade Representative has consistently identified inadequate trade secret protection in China and other nations as a significant structural barrier for American manufacturers operating in those markets.⁴⁹ Manufacturing trade secrets relating to advanced materials, precision components, and process technology are priority targets for state-directed acquisition programs because they underpin both commercial competitiveness and defence industrial capacity. IP-intensive manufacturing industries collectively generate 41 per cent of the

⁴⁶Insulet Corp v EOFlow Co Ltd, WilmerHale Trade Secret Update (n 49) 5-6; Federal Circuit panel comprising Judges Lourie, Prost and Stark.

⁴⁷TFL, 'Trade Secret Litigation Activity is on the Rise' (The Fashion Law, 25 April 2020) <<https://www.thefashionlaw.com/trade-secret-litigation-activity-is-on-the-rise/>> accessed 20 April 2026.

⁴⁸PPG Industries v Jiangsu Tie Mao Glass Co, 47 F 4th 156 (3d Cir 2022); WilmerHale (n 49) 4.

⁴⁹USTR, 2023 Special 301 Report (n 41) 12-13; USTR, 2025 Special 301 Report 4-5.

United States GDP and directly employ 47.2 million workers,⁵⁰ meaning that the erosion of trade secret protection in this sector carries direct consequences for employment, export competitiveness, and national security.

D. Financial Services

The financial services sector presents a distinctive profile in which the primary trade secrets are not technical processes or formulations but rather proprietary financial models, trading algorithms, customer relationship data, and business intelligence. The sector's misappropriation cases frequently arise in the context of employee departures to competing institutions, where the information transferred consists of client lists, pricing matrices, and analytical methodologies that represent the core of the departing employee's commercial value to their new employer.

The 2023 collapse of Silicon Valley Bank generated a paradigmatic financial services trade secret case. Following First Citizens BancShares' acquisition of SVB's deposits and loans, 42 former SVB technology and life sciences bankers left First Citizens to join HSBC within weeks. First Citizens filed a \$1 billion lawsuit alleging misappropriation of trade secrets, including customer relationship data, institutional knowledge, and proprietary business strategies developed during the bankers' tenure at SVB.⁵¹ The case illustrates the particular difficulty of protecting trade secrets in the financial services sector, where the commercial value of proprietary information is inseparable from the expertise of the individuals who hold it, and where the law must navigate the boundary between employees' right to use their general skills and the firm's right to protect genuinely proprietary information about its clients and strategies.

Lex Machina's 2024 Trade Secret Litigation Report identified financial institutions and insurance companies as the most active plaintiffs in federal trade secret cases over the 2021 to 2023 period,⁵² reflecting both the sector's heightened awareness of trade secret risk and its willingness to litigate aggressively to deter competitor poaching of both personnel and proprietary information. The sector's litigation activity also reflects the structural tension between the economic value of customer relationships, which the law recognises as protectable trade secrets in appropriate circumstances, and employees' legitimate interest in maintaining their professional networks and reputations in a career that depends upon personal relationships with clients.

⁵⁰IP-intensive industries generate 41% of US GDP and employ 47.2 million workers directly: USTR (n 58); USPTO, *Intellectual Property and the US Economy* (2022).

⁵¹First Citizens BancShares v HSBC Holdings plc et al, No 3:23-cv-02836 (ND Cal), complaint filed June 2023.

⁵²Lex Machina (n 23) 6-7; financial institutions and insurance companies cited as most active plaintiffs 2021-2023.

5. Direct Microeconomic Impacts on United States Firms

The economic analysis of trade secret misappropriation at the firm level requires disaggregating the aggregate estimates discussed in Sections II and IV into their constituent components: the direct financial losses that misappropriation imposes on the victim firm, the secondary costs that misappropriation generates independently of the direct revenue loss, and the structural distortions that misappropriation introduces into the firm's investment incentives and strategic behaviour. Each category of harm is economically distinct, operates across a different time horizon, and raises different questions about the adequacy of the legal remedies available to victimised firms under the Defend Trade Secrets Act and its state analogues.

A. Revenue Loss, Market Share Erosion, and Competitive Acceleration

The most immediate and direct microeconomic consequence of trade secret misappropriation is the loss of revenue that the stolen information would have generated had it remained exclusively under the victim's control. This loss operates through two distinct channels. First, the mis appropriator obtains a competitive advantage by eliminating the development costs it would otherwise have incurred to achieve the same technological or commercial position, allowing it to price its products more aggressively or to capture market share that would otherwise have flowed to the victim. Second, the victim's competitive position is directly undermined because the proprietary information that previously differentiated its products from those of competitors has been transferred to those competitors, accelerating the pace at which market contestability erodes the victim's pricing power.

Recent empirical evidence from a Harvard Working Paper by Kao and Tadepalli, compiling publicly disclosed espionage incidents from 1995 to 2024, provides the most rigorous quantitative evidence to date of these effects at the firm level. The study found that, in an event-study design, revenues at targeted firms declined by approximately 40 per cent within five years of a successful espionage incident, with effects persisting for up to a decade.⁵³ Equally significant, R&D expenditure at targeted firms declined by approximately 40 per cent over the same five-year period.⁵⁴ This dual compression of revenue and R&D investment represents a self-reinforcing cycle of competitive decline: the misappropriation erodes the victim's market position, which reduces its cash flows, which in turn constrains its capacity to invest in the next generation of proprietary technology that might restore its competitive standing.

⁵³Andrew Kao and Karthik Tadepalli, "Economic Espionage and Innovation Restrictions" Harvard Working Paper (December 2025) 1, 3.

⁵⁴*ibid* 3-4.

Figure 9. Direct Microeconomic Impacts on U.S. Firms from Trade Secret Misappropriation
 Sources: Kao & Tadeipalli (2025); HBR / Eureka (2024); IBM (2023); Ponemon (2026)

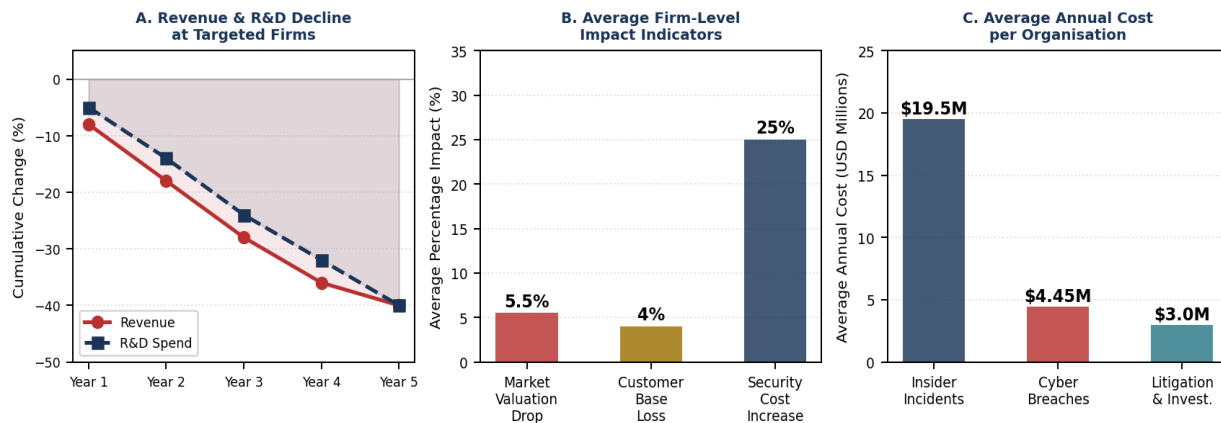


Figure 9. Direct Microeconomic Impacts on U.S. Firms from Trade Secret Misappropriation Sources: Kao & Tadeipalli (2025); HBR / Eureka (2024); IBM (2023); Ponemon (2026)

The stock market provides an additional signal of the severity of these effects. A study referenced in the Harvard Business Review found that trade secret theft results in an average 5 to 7 per cent drop in market valuation for publicly traded companies as shareholders react to perceived competitive vulnerability and revised revenue expectations.⁵⁵ This valuation decline is particularly significant because it is forward-looking; it reflects not only the direct loss of current revenue but the market's assessment of the long-term impairment of the firm's competitive position. The loss of customer trust compounds the financial harm: research by the Ponemon Institute found that companies can lose up to 4 per cent of their customer base in the aftermath of an IP-related data breach.⁵⁶

B. Reactive Security and Compliance Expenditure

A second category of direct microeconomic impact consists of the reactive expenditures that misappropriation forces upon victimized firms. These costs are distinct from the revenue losses described above because they represent real resource commitments by the firm that generate no productive output; they are pure deadweight losses from the firm's perspective, representing capital diverted from investment in productive activity to defensive security infrastructure.

Following the discovery of misappropriation, companies typically undertake substantial investments in cybersecurity infrastructure upgrades, forensic investigation costs, employee monitoring and audit systems, enhanced access controls, and legal counsel for both the investigation and any resulting litigation. Research suggests that companies experiencing trade secret theft increase their security expenditure by an average of

⁵⁵Eureka Software, "The Economic Impact of Trade Secret Theft on Businesses" (14 November 2024), citing Harvard Business Review study.

⁵⁶ibid; Ponemon (n 37) 4.

25 per cent in the year following discovery.⁵⁷ The Ponemon Institute's 2026 report found that the average annual cost of insider-related incidents, which encompass the full spectrum of detection, investigation, containment, and remediation activities, now stands at \$19.5 million per organisation, representing a 123 per cent increase from \$8.76 million in 2018.⁵⁸ When added to the average cost of a cyber breach at \$4.45 million and baseline litigation costs of \$3 million per case,⁵⁹ the aggregate security and compliance burden on firms actively managing trade secret risk is substantial, representing a structural tax on innovation-intensive activity that has no counterpart in industries where competitive advantage rests on publicly available information.

C. Investment Distortions and Chilling Effects on R&D

The most economically significant microeconomic impact of trade secret misappropriation operates not at the level of the firm that has already been victimised but at the level of the broader population of firms that rationally adjust their behaviour in anticipation of the risk of misappropriation. This chilling effect on R&D investment is the central concern of the economic paradox identified by Buccafusco, Masur, and Varadarajan in their 2025 analysis of the trade secrecy information paradox.⁶⁰ When firms cannot be confident that the legal framework will provide adequate compensation for the misappropriation of their R&D investment, they face a rational incentive to reduce that investment to the level that can be protected through secrecy alone, rather than the level that would maximise social welfare.

The Kao and Tadepalli study provides direct empirical evidence of this chilling effect. In addition to documenting the 40 per cent decline in R&D spending at targeted firms, the study examined whether firms restrict knowledge sharing in response to espionage, finding evidence that victimised firms adopt more secretive behaviours in their innovation processes, reducing both the quantity and the collaborative character of their research activity.⁶¹ This finding is economically significant because it suggests that the harm of trade secret misappropriation extends beyond the direct value of the information stolen to the systemic reduction in the productive efficiency of the innovation process that results when firms respond to misappropriation risk by internalising information that would otherwise flow freely through the economy.

The legal framework responds to this chilling effect through the provision of exemplary damages for willful and malicious misappropriation under both the DTSA and most state analogues, which permit courts to award up to double the compensatory damages where the defendant's conduct is found to be intentional and

⁵⁷ Tangibly, 'The Financial Impact of Trade Secret Misappropriation' (Tangibly, 8 January 2026) <https://www.tangibly.com/the-financial-impact-of-trade-secret-misappropriation/> accessed 20 April 2026.

⁵⁸ Ponemon Institute, 2026 Cost of Insider Risks Global Report (Ponemon Institute/DTEX 2026) <https://ponemon.dtex.ai/> accessed 8 April 2026.

⁵⁹ Ibid

⁶⁰ Buccafusco, Masur and Varadarajan (n 16) 927-928.

⁶¹ Ibid 4-5.

egregious. The availability of exemplary damages is theoretically important because it is designed to price misappropriation above its expected return, thereby deterring rational actors who would otherwise treat the risk of detection-adjusted liability as an acceptable cost of competitive behaviour. However, the empirical evidence documented by Kao and Tadepalli suggests that the deterrent effect of the current damages regime remains incomplete, particularly in the context of state-sponsored misappropriation, where foreign state actors are effectively immune from the United States civil and criminal process.

D. Litigation Costs and the Economics of Enforcement

The direct economic costs of enforcing trade secret rights through litigation represent a fourth category of firm-level impact. As noted in Section III, trade secret litigation costs range from \$50,000 at the preliminary injunction stage to \$1-5 million at trial and \$25 million or more in complex high-stakes cases.⁶² These costs are borne not only by victimised firms but by alleged misappropriators, creating substantial bilateral deterrence from litigation that may explain the significant gap between the number of misappropriation incidents that Tim Londergan of Tangibly estimated at potentially 100 times the number of cases filed, and the approximately 1,200 to 1,400 cases actually filed in federal courts each year.⁶³

6. Macroeconomic Consequences for the United States

The microeconomic harms documented in Section V start to add up into broader macroeconomic consequences that ripple across the United States economy's ability to innovate, stay internationally competitive, keep its employment base steady, and maintain long term productivity growth. But getting a clean read on these overall effects is, frankly, more difficult than measuring firm-level impacts, because they travel through multiple channels at the same time, rely on very tangled counterfactual thinking about what the economy would have produced if the misappropriation had not happened, and they run straight into the measurement problem flagged by the IP Commission. In many cases, companies do not even know their trade secrets have been taken, and the ones that do sometimes are also, reluctant to come forward and disclose the fact.⁶⁴ Nevertheless, the evidence assembled by the IP Commission, the United States Senate, the Office of the Director of National Intelligence, and recent academic research provides a coherent and mutually reinforcing picture of macroeconomic damage of significant scale.

⁶² American Intellectual Property Law Association, *2025 Report of the Economic Survey* (AIPLA 2025) <<https://www.aipla.org/home/news-publications/economic-survey/2025-report-of-the-economic-survey> accessed 7 May 2026.>

⁶³Londergan, Tangibly (n 47); Almeling (n 26) 291.

⁶⁴IP Commission Report (n 18) 1-2.

Figure 10. Macroeconomic Aggregate Consequences of Trade Secret Misappropriation (United States)
 Sources: IP Commission Report (2017); PwC/CREATe (2014); ODNI (2018); Kao & Tadepalli (2025); US Senate DTSA Report (2016)

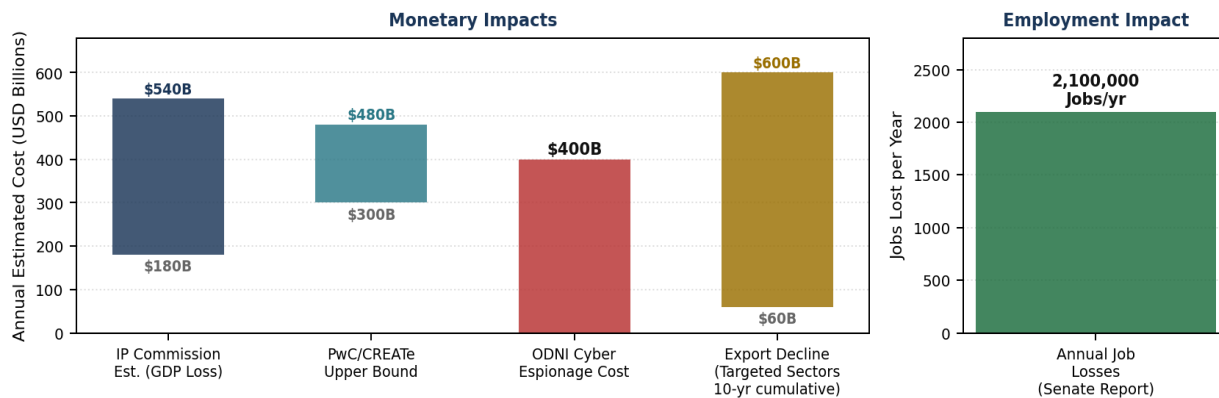


Figure 10. Macroeconomic Aggregate Consequences of Trade Secret Misappropriation (United States)
 Sources: IP Commission Report (2017); PwC/CREATe (2014); ODNI (2018); Kao & Tadepalli (2025); US Senate DTSA Report (2016)

A. GDP and Innovation Output

The most direct macroeconomic consequence of trade secret misappropriation is the reduction in aggregate innovation output that results from the chilling effects on R&D investment documented at the firm level. The IP Commission estimated that trade secret theft costs between one and three per cent of GDP annually, representing a range of \$180 billion to \$540 billion at the time of the report's 2017 update.⁶⁵ The PwC/CREATe study, cited in the United States Senate's report on the DTSA, placed the annual cost at up to \$480 billion.⁶⁶ These estimates, while representing the most comprehensive attempts to quantify the aggregate harm, are acknowledged by their authors to be conservative because they do not fully capture the second-order effects of reduced R&D investment on the pace of technological progress.

The Kao and Tadepalli study provides the most methodologically rigorous recent estimate of the aggregate macroeconomic consequences. Their event-study analysis found that exports in sectors targeted by espionage declined by 60 per cent over a decade, reflecting the structural erosion of the United States' comparative advantage in the advanced technology industries that are the primary targets of state-sponsored misappropriation.⁶⁷ This export decline represents a direct and sustained loss of national income that operates through the balance of payments rather than through domestic consumption. It is not merely a redistribution of economic activity from one firm to another; it represents a genuine reduction in the global market share

⁶⁵IP Commission Report (n 18) 2; PwC/CREATe (n 21) 6.

⁶⁶PricewaterhouseCoopers LLP and Center for Responsible Enterprise and Trade, *Economic Impact of Trade Secret Theft* (2014) 6, cited in US Senate Report (n 19) 3.

⁶⁷Kao and Tadepalli (n 63) 5.

of United States firms in sectors that have historically been the primary source of the country's trade surplus in high-technology goods and services.

B. Employment and Wage Effects

The United States Senate's report on the Defend Trade Secrets Act stated that trade secret theft has led to the loss of 2.1 million American jobs each year,⁶⁸ a figure that reflects both the direct employment consequences of misappropriation, as victimised firms lose revenue and reduce their workforces, and the indirect consequences through the suppression of the R&D investment that generates employment in innovation-intensive industries. IP-intensive industries collectively employ 47.2 million workers directly and generate employment for tens of millions more in supplier and service industries.⁶⁹ Workers in IP-intensive industries also enjoy pay that is, on average, 60 per cent higher than workers in other sectors,⁷⁰ meaning that the displacement of employment from IP-intensive to less IP-intensive sectors caused by trade secret misappropriation entails not only a reduction in the quantity of employment but a reduction in its quality, measured by wage level and associated benefits.

The employment consequences of trade secret misappropriation also operate through the channel of business exit. When a firm loses its primary trade secrets, particularly in the pharmaceutical or advanced manufacturing sectors where those secrets represent years of irreplaceable R&D investment, the economic viability of the firm may be fundamentally compromised. Business exit is not captured in standard estimates of misappropriation costs, but it represents a particularly severe form of economic harm because it eliminates not only current employment but the future innovation capacity that the exiting firm would have generated.

C. Innovation Ecosystem and Long-Run Productivity

The most economically significant but least quantifiable macroeconomic consequence of trade secret misappropriation, kind of works through its long run effects on how the United States innovation ecosystem is structured. As mentioned in Section II, the trade secret regime seems to contain this core economic paradox: it is set up to incentivise the production of socially valuable knowledge by letting firms capture private returns from their R&D, while misappropriation of that knowledge by rivals creates a social loss. And that happens because it discourages the very investment that generated it, in the first place.

When trade secret misappropriation is systematic rather than episodic, it distorts the allocation of R&D investment across the economy in two ways that are mutually reinforcing. First, as documented by Kao and Tadepalli, victimised firms reduce their R&D expenditure in response to misappropriation, contracting the

⁶⁸US Senate Report (n 19) 2.

⁶⁹USPTO, Intellectual Property and the U.S. Economy: Third Edition (USPTO 2022) 2 uspto.gov accessed 7 April 2026.

⁷⁰USTR (n 58) 4-5; US Senate Report (n 19) 2-3.

supply of new proprietary technology.⁷¹ Second, firms that have not yet been victimised but perceive an elevated risk of misappropriation rationally shift their investment portfolios toward less knowledge-intensive activities where their returns are less vulnerable to misappropriation, further reducing the aggregate supply of innovative activity.

D. The Underreporting Problem and True Scale of Economic Harm

Any assessment of the macroeconomic consequences of trade secret misappropriation must grapple seriously with the underreporting problem identified by the IP Commission and subsequent analysts. The Commission offered three explanations for why standard assessments systematically underestimate the scale of harm. First, many firms do not maintain adequate trade secret inventories and therefore do not know when their secrets have been stolen. Second, firms that do know are often reluctant to disclose the fact, both because disclosure itself may further erode the competitive value of the stolen information and because of the reputational consequences of admitting that security has been breached. Third, the civil and criminal enforcement process captures only a fraction of actual misappropriation incidents; the Tangibly analysis cited in Section III estimated that the true number of misappropriation incidents may be 100 times the number of cases filed.⁷²

The legal-economic implication of underreporting is that the aggregate damages regime established by the DTSA significantly underprices misappropriation relative to its true social cost. When compensatory damages are calibrated to the losses and gains documented in the fraction of incidents that actually result in litigation, the expected liability facing a rational misappropriator is far below the expected value of the information obtained. This systematic underpricing of misappropriation is not merely a theoretical concern; it has structural consequences for the deterrence function of the legal framework, creating persistent incentives for misappropriation that the current enforcement system is structurally unable to eliminate.

The overall evidence points to a conclusion that is economically significant, and also legally important at the same time. Trade secret misappropriation puts costs onto the United States economy that are substantial in absolute terms, persistent in duration, and systemic in how they ripple across the innovation ecosystem that produces the country's long-run comparative advantage. The legal framework set out by the DTSA along with its state analogues counts as a real upgrade compared to the balkanized common law regime that came before it, but there's still a gap between what the framework can deter in practice, and the actual scale of misappropriation happening in the real world. That mismatch implies that more reform is needed. What those reforms are like, and which principles should guide their development, is what the next section is about.

⁷¹ibid 5-6.

⁷² Tangibly (n70)

7. Policy Recommendations and Future Outlook

The foregoing analysis has established that trade secret misappropriation inflicts economic harm on the United States which is huge in absolute magnitude, lasting for a long time, and kind of systemic in how it affects the innovation ecosystem. The legal framework that came from the Economic Espionage Act of 1996 and the Defend Trade Secrets Act of 2016 is, in a sense a genuine and significant improvement over the fragmented common law regime that was there before, but the evidence reviewed across the preceding sections kind of discloses three structural deficiencies that the present framework has not resolved, or at least not fully.

First, the damages regime systematically underprices misappropriation relative to its true social cost, because the expected civil and criminal liability facing a rational misappropriator is calibrated to the fraction of incidents that result in detected and litigated cases rather than to the full population of incidents that actually occur.

Second, the enforcement architecture really ends up creating sharp access-to-justice inequalities, and it feels like smaller and medium-sized enterprises are left without real remedies, even though they carry the same misappropriation risk as big corporations. Third, the extraterritorial reach of the current framework is kind of inadequate, mainly because the most economically significant kind of misappropriation is state-sponsored economic espionage, and foreign state actors usually operate way beyond the effective reach of United States civil and criminal procedure. So, this section then pushes forward a group of policy recommendations meant to tackle each one of those structural gaps, and it also wraps up by looking at the emerging challenges that will shape trade secret law and day-to-day practice over the next decade.

A. Recalibrating the Damages Regime

The most important reform that Congress and the courts can realistically make is a recalibration of the damages setup, so it lines up with the real social cost of misappropriation not just the directly measurable harm that happens in the particular case that gets litigated. The existing framework, which allows compensatory damages to be calculated either by the victim's own actual loss, or by the misappropriator's unjust gain, and then adds exemplary damages that can reach as much as double the compensatory amount for wilful and malicious behavior, was meant to put harmed firms back on their feet and also to deter a rational wrongdoer. Still, the Tangibly analysis, along with the wider empirical work, suggests that the mix of severe underreporting, costly litigation and the built-in practical impossibility of finding many kinds of cyber enabled misappropriation means that the expected liability hanging over a misappropriator ends up being only a small slice of the expected value of the information that was obtained.

Congress ought to look at two complementary ways to close this gap, and really, it's sort of the same idea in

a different dress. First, Congress could add a statutory minimum damages provision for trade secret misappropriation, sort of like the statutory damages setup you see in copyright law under 17 USC section 504. That framework would let courts award a minimum amount per misappropriated trade secret, without forcing the harmed party to prove the entire size of its actual loss. These minimum damages tool would be especially helpful for small and medium sized enterprises, because they often do not have the money or time to hire the expert economic testimony that's needed to pin down an exact damages number at trial, and then everyone just waits.

The second mechanism is a mandatory disgorgement remedy for willful misappropriation. This one will require the mis appropriator to disgorge each and every profit derived from the stolen information, even if those profits are more than the victim's provable loss. A disgorgement remedy, when treated as mandatory, would help fix the structural asymmetry that was identified in Kao and Tadepalli's study, where the mis appropriator captures substantially more value from the stolen information than the victim loses on direct revenue, because the mis appropriator dodges the development costs that the victim had and can price its products accordingly.

Strengthening Access to Justice for Small and Medium-Sized Enterprises

The second structural deficiency in the current framework is, the access-to-justice inequality that effectively denies SMEs viable enforcement remedies even when the merits of their trade secret claims are strong. The Tangibly analysis estimated that filing a federal trade secret case requires between \$50,000 and \$250,000 in upfront costs, and that it rises to \$1 to 5 million at trial. For a small technology firm or pharmaceutical startup whose primary asset is a proprietary process or formulation, this cost structure means that the rational response to misappropriation is often forbearance rather than enforcement, especially when the defendant is a well-capitalized corporation that can outspend the plaintiff at every stage, of the litigation.

Two reforms should be considered. First, Congress should establish a federal trade secret small claims mechanism, modelled on the framework of the Copyright Claims Board created by the CASE Act of 2020,⁷³ that would allow SMEs to bring misappropriation claims in a streamlined administrative forum with capped filing fees, simplified discovery procedures, and damages capped at a level proportionate to the scale of the typical SME case. Such a mechanism would not replace the full federal court framework for large-scale misappropriation but would create a realistic enforcement pathway for the substantial number of cases that currently go unenforced due to the prohibitive economics of federal litigation.

Second, the DTSA⁷⁴ should be amended to require courts to award reasonable attorneys' fees to prevailing

⁷³ CASE Act of 2020, Pub L 116-260

⁷⁴ DTSA 18 USC s 1836(b)(3)(D) (current attorneys' fees provision, limited to bad-faith claims)

plaintiffs in cases involving wilful misappropriation so as to reverse the current default that each party bears its own legal costs. Fee-shifting in wilful misappropriation cases would substantially reduce the cost differential between large and small litigants and would deter the strategic use of superior litigation resources to exhaust smaller plaintiffs before trial.

Addressing State-Sponsored Misappropriation

The third and most challenging structural deficiency is the inadequacy of the existing framework to address state-sponsored economic espionage. As documented, the Office of the Director of National Intelligence estimated that economic espionage through cyber intrusion costs the United States \$400 billion annually, a figure that dwarfs the aggregate value of all civil trade secret awards in the history of the DTSA. Yet the fraction of this harm that is redressed through either criminal prosecution under the Economic Espionage Act or civil litigation is vanishingly small, because foreign state actors are effectively immune from the United States judicial process, and the evidentiary requirements for establishing state-attribution in both criminal and civil proceedings are extremely demanding.

The most promising avenue for reform is the expansion and systematic use of executive branch tools that do not depend on judicial enforcement against foreign defendants. The Protecting American Intellectual Property Act of 2022 established a framework for mandatory sanctions against foreign individuals and entities identified as perpetrators of significant trade secret theft from United States firms, and represents a meaningful complement to the criminal enforcement framework of the EEA. Congress should strengthen this framework by establishing an automatic sanction mechanism triggered by indictment under section 1831 of the EEA, eliminating the current requirement for a separate executive determination, and extending the sanctions reach to the state-owned enterprises and financial institutions that benefit from state-sponsored misappropriation, even where the state actors themselves cannot be reached. At the international level, the United States should pursue bilateral and multilateral trade agreements that establish enforceable minimum standards for trade secret protection and require trading partners to establish criminal penalties that are calibrated to deter state-directed misappropriation rather than merely retail IP theft.

Future Outlook: Artificial Intelligence, Algorithmic Trade Secrets, and Emerging Challenges

The legal and economic landscape of trade secret protection is being reshaped by the rapid development of artificial intelligence and machine learning technologies. These developments create both new categories of protectable trade secrets and new mechanisms of misappropriation that existing legal frameworks were not designed to address. Training data, model weights, fine tuning methodologies, and inference architecture are all potentially protectable trade secrets under the broad definition of protected information in the Defend Trade Secrets Act . The commercial value of these assets in the most advanced artificial intelligence systems

substantially exceeds that of conventional software source code. The misappropriation of algorithmic trade secrets therefore represents a category of harm that, if unaddressed, could transfer the primary economic benefits of United States leadership in artificial intelligence to foreign competitors that acquire proprietary model assets through espionage rather than investment.⁷⁵

The distinctive challenge that artificial intelligence trade secrets present for the legal framework is the difficulty of identifying the boundaries of the protected information with sufficient precision. This precision is necessary to satisfy the specificity requirements that courts have consistently enforced since the enactment of the Defend Trade Secrets Act. A training dataset consisting of hundreds of billions of tokens or a neural network with hundreds of billions of parameters does not map cleanly onto the conception of a bounded and identifiable trade secret that the uniform and federal statutes were designed to protect. There is an urgent need for courts to craft new models of analysis to resolve disputes involving the use of algorithms. The models should be able to single out the particular elements of a model or database that gain separate economic value through secrecy without granting immunity to misappropriation or making the protection too broad and inclusive of public information used in a training database.

The growing intersection of trade secret law and employment law presents a further emerging challenge. The Federal Trade Commission proposed rule banning non compete agreements reflects a broader policy trajectory toward enhanced employee mobility, even though it was subsequently challenged in federal courts.⁷⁶ This trajectory will likely increase the rate of insider misappropriation because it eliminates the principal contractual mechanism through which firms currently deter departing employees from commercialising proprietary information at competing enterprises.

As jurisdictions progressively restrict non-compete enforcement, the duty of protection will slide more and more onto trade secret law itself. In practice this shift will force courts to define where protectable trade secrets end and where the general skills and know how that employees are allowed to take with them from employer to employer begin. That definitional puzzle will probably be hardest in technology and pharmaceutical sectors. There the line between an employee's general expertise and a firm's specific proprietary methodology gets blurred almost by default, because the work is knowledge intensive in nature.

Taken together, these developing changes raise both the economic risks tied to trade secret protection and the overall legal complexity of trying to secure it. Since the Defend Trade Secrets Act was enacted in 2016, the path of the law has been broadly positive. Litigation volume has climbed, damages awards have gotten bigger, and federal courts have built up a pretty substantial body of doctrine around the major parts of the

⁷⁵ Wilmer Hale, 2024 Trade Secret Update (2024) 1

⁷⁶ Non-Compete Clause Rulemaking 89 Fed Reg 38342 (May 2024); *Ryan LLC v FTC* 2024 WL 3879954 (ND Tex 2024)

statute. Still, the speed at which the law is developing seems to trail behind the speed of technological change. The structural gaps highlighted in this analysis indicate that unless Congress, the courts, and the executive branch coordinate their efforts to recalibrate the framework, the distance between what the law hopes to do and what it actually achieves will keep widening into the coming decade.

Reference

Table of Cases

Appian Corp v Pegasystems Inc, Case No 1399-22-4 (Court of Appeals of Virginia, argued November 2023)

Computer Sciences Corp v Tata Consultancy Services Ltd, No 3:15-CV-01187 (ND Tex), jury verdict November 2019

First Citizens BancShares v HSBC Holdings plc et al, No 3:23-cv-02836 (ND Cal), complaint filed June 2023

Insulet Corp v EOFlow Co Ltd, Federal Circuit panel comprising Judges Lourie, Prost and Stark

Motorola Solutions Inc v Hytera Communications Corp, No 1:17-cv-01973 (ND Ill), jury verdict February 2020, reduced to \$544 million on appeal

Peabody v Norfolk 98 Mass 452 (1868)

PPG Industries v Jiangsu Tie Mao Glass Co, 47 F 4th 156 (3d Cir 2022)

Ryan LLC v FTC 2024 WL 3879954 (ND Tex 2024)

Syntel Sterling Best Shores Mauritius Ltd v The TriZetto Group Inc, verdict October 2020 (SDNY)

TF Global Markets Ltd v Sorenson, 2023 US Dist Lexis 27983 (ND Ill, 17 February 2023)

Versata Software, Inc v Ford Motor Company (2023)

Table of Legislation

CASE Act of 2020, Pub L 116-260

Defend Trade Secrets Act of 2016, 18 USC § 1836

Economic Espionage Act of 1996, 18 USC §§ 1831-1839

Non-Compete Clause Rulemaking 89 Fed Reg 38342 (May 2024)

Protecting American Intellectual Property Act of 2022

Uniform Trade Secrets Act 1979

Secondary Sources

Books and Reports

- American Intellectual Property Law Association, *2025 Report of the Economic Survey* (AIPLA 2025)
- Commission on the Theft of American Intellectual Property, *IP Commission Report: The Theft of American Intellectual Property* (National Bureau of Asian Research, Update 2017)
- Congressional Research Service, *Stealing Trade Secrets and Economic Espionage: An Overview of the Economic Espionage Act*, R42681 (29 October 2024)
- Doyle C, *Stealing Trade Secrets and Economic Espionage: An Abridged Overview of the Economic Espionage Act* (Congressional Research Service Report R42682 2024)
- Goudkamp J and Nolan D, *OSCOLA: The Oxford University Standard for Citation of Legal Authorities* (5th edn, Hart Publishing 2026)
- IBM Security, *Cost of a Data Breach Report 2023* (IBM 2023)
- Lex Machina, *2024 Trade Secret Litigation Report* (LexisNexis 2024)
- National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (ODNI 2018)
- Ocean Tomo LLC, *Annual Study of Intangible Asset Market Value* (2015)
- Office of the Director of National Intelligence, *Foreign Economic Espionage in Cyberspace* (2018)
- Ponemon Institute, *2026 Cost of Insider Threats: Global Report* (Proofpoint 2026)
- PricewaterhouseCoopers LLP and Center for Responsible Enterprise and Trade, *Economic Impact of Trade Secret Theft* (2014)
- Stout, *2024 Trends in Trade Secret Litigation Report* (Stout 2024)
- US Senate, *Report on the Defend Trade Secrets Act of 2016*, S Rep No 114-220, 114th Cong, 2nd Sess (2016)
- USPTO, *Intellectual Property and the US Economy: Third Edition* (USPTO 2022)
- USTR, *2023 Special 301 Report* (2023)
- USTR, *2025 Special 301 Report* (2025)
- WilmerHale, *2024 Trade Secret Update: A Look at Recent Trade Secret Developments and Trends* (19 July 2024)
- WIPO, *Guide to Trade Secrets and Innovation, Part V* (2024)

Journal Articles

Almeling DS and others, 'A Statistical Analysis of Trade Secret Litigation in Federal Courts' (2010) 45 Gonzaga L Rev 291

Buccafusco C, Masur JS and Varadarajan D, 'Trade Secrecy Information Paradox' (2025) 100 Notre Dame L Rev 925

Dhanol J and Kashyap PK, 'A Comparative Analysis of Trade Secret Protection in the USA, UK, Australia, and India' (2024) 30 Educational Administration: Theory and Practice 6654

Nashkova S, 'Defining Trade Secrets in the United States Past and Present Challenges A Way Forward' (2023) 54 IIC 634

ScienceDirect, 'Trade secrets and cyber security breaches' (2022) 8 Journal of Finance and Data Science 202

Working Papers

Kao A and Tadepalli K, 'Economic Espionage and Innovation Restrictions' Harvard Working Paper (December 2025)

Blog Posts and Online Articles

Economist Intelligence Unit, 'Open secrets? Guarding value in the intangible economy' (9 June 2021)

Eureka Software, 'The Economic Impact of Trade Secret Theft on Businesses' (14 November 2024)

Londergan T, 'The Invisible Epidemic: Unprosecuted Trade Secret Theft' *Tangibly* (19 November 2025)

Morningstar S, 'Trade Secret Theft Trends: A Closer Look at the Perpetrators' *The Cipher Brief* (5 June 2024)

Pfeffer W and Deol H, 'How to Protect Precious IP from Layoff-Related Insider Theft' *Corporate Compliance Insights* (7 June 2023)

Pooley J, 'The US Defend Trade Secrets Act Eight Years On' *IAM Trade Secrets Blog* (14 May 2024)

Tangibly, 'The Financial Impact of Trade Secret Misappropriation' (8 January 2026)

Industry and Committee Reports

Carrier Management, 'Report: Bump in Federal Trade Secret Litigation Seen in 2023' (17 September 2024)

International Bar Association Health and Life Sciences Committee, 'Trade secrets: a strategic element in the life sciences and biotechnology industries' (2024)

Kirkland and Ellis, Trade Secret Litigation Report (2024)

Frontiers in Bioengineering and Biotechnology (2019), citing Research America (2016)